

中存储日志信息。“/var/log/auth.log”或“/var/log/secure”文件存储来自可插入身份认证模块(PAM)的日志,包括已成功的登录、失败的登录尝试和认证方式等。Ubuntu 和 Debian 在“/var/log/auth.log”文件中存储认证信息,而 RedHat 和 CentOS 则在“/var/log/secure”文件中存储该信息。

多数基于 Linux 环境的应用程序都提供了功能丰富的日志记录,用于记录主要事件与出错信息,以加强对程序运行的监管。例如,Apache 程序的访问日志(access log)记录了 HTTP 访问的相关信息,通过漏洞扫描可以从中发现系统存在的安全缺陷,通过对这些安全缺陷的利用就可以达到远程入侵的目的。

3.3 Linux 系统的远程攻防技术

与针对 Windows 系统的攻防相似,针对 Linux 系统的网络攻防技术同样包括收集目标 Linux 主机的信息、发现安全漏洞、利用安全漏洞远程获取 Linux 主机的 Shell 访问权、提权至 Root 用户权限、实施攻击行为等步骤。本节主要介绍各个步骤的主要实现方法。

3.3.1 Linux 主机账户信息的获取

由于 Linux 系统所具有的可靠性和稳定性,互联网上的 FTP、邮件、Web 等大量的应用服务多采用 Linux 系统来提供。针对这些应用服务的网络攻击,多通过收集目标主机的远程登录账户信息(用户名+口令)来实现。

1. 远程登录账户信息的获取

获取远程登录用户的账户信息是实施远程入侵的关键,为此,攻击者在确定了被攻击的目标后,需要通过各种方法获得登录的用户名和密码。为实现这一目的,最高效的办法是在直接获取保存远程登录账户信息的文件(/etc/passwd 和 etc/shadow)后,从文件中取得用户名和密码。很显然,这一过程是很难实现的,因为出于安全考虑,Linux 系统对保存用户账户信息的文件从存储和访问控制等方面都设置了严格的管理权限,只有 Root 用户才能读取,而要获取 Root 用户的权限则需要获得其密码。

在具体网络攻防中,多通过口令猜测或暴力破解等攻击手段来获取远程登录账户的信息。一般过程是:先利用 Linux 系统上的 rusers、sendmail、finger 等服务来获取被攻击 Linux 主机上的用户名;然后再通过猜测(针对弱口令)、字典攻击、暴力破解等方式来获得对应的密码。其中,由于 Root 账户的重要性,利用该方法获得其登录密码几乎成为所有攻击者的关注目标。

除了系统账户信息外,HTTP/HTTPS、FTP、SNMT、POP3/SMTP、MySQL 等基于 Linux 系统的各类网络服务所拥有的管理账户信息也是攻击者关注的焦点。不过,与系统账户不同的是,这些网络服务的管理账户的操作一般会被限制在一定的范围之内。例如,Apache 是 Linux 系统上使用最为广泛的 HTTP 服务,攻击者在获得管理员账户信息后,就可以对发布的 Web 站点目录文件进行读取或修改,利用可以上传 PHP 后门程序的权限,达到修改 Web 主页或上传木马的目的。

2. 远程登录账户的防范方法

与 Windows 系统中用户账户信息的安全管理类似,在 Linux 系统中要防御针对远程登录账户的攻击,仍然需要从用户名和密码两方面入手,加强对用户账户信息的管理。主要包括以下几方面。

- (1) 为不同的管理员分配不同的管理账户,而不是共同使用 Root 账户。
- (2) 限制 Root 等特权账户的远程登录功能,只允许其本地登录。如果部分特权账户需要进行远程登录,可使用普通账户登录后再通过 su 命令提权,su 命令的密码功能可以增强登录账户的安全性。
- (3) 限制尝试登录次数,对多次登录失败的账户进行锁定并记录其信息。
- (4) 密码设置符合复杂性要求,即密码不少于 8 个字符,字符包含字母、数字和特殊符号(如 \$、@、_ 等)。

最有效的安全防范方法是利用基于 PKI(Public Key Infrastructure,公钥密钥基础设施)技术的身份认证机制来替代传统的“用户名+口令”方式,同时将一些安全风险较高的服务(如 SSH)设置到非熟知端口上,以减少口令攻击的可能性。

3.3.2 Linux 主机的远程渗透攻击

远程渗透攻击的实现主要依赖于目标主机上存在的各类安全漏洞。所以,当攻击者要对某一目标主机进行远程渗透攻击前,首先要收集目标主机的相关信息,并分析是否存在安全漏洞。如果存在安全漏洞,才考虑如何去利用。为此,从攻防角度分析,发现安全漏洞是实施攻击的前提,而及时修补安全漏洞是进行防范的基础。

1. Linux 安全漏洞及利用

漏洞的普遍性及其后果的严重性促使研究人员将更多注意力集中于漏洞相关技术的研究上,包括漏洞检测(发现/挖掘)、漏洞特性分析、漏洞定位、漏洞利用、漏洞消控等。Linux 作为一个开放源代码的操作系统,较之闭源的 Windows 操作系统,研究人员可以从源代码分析过程中发现漏洞,并利用其开源性进行及时修复。然而,也存在一些漏洞在发现之后未能及时发布补丁程序,而是被用于渗透攻击的现象。

与 Windows 系统相比较,Linux 系统的安全漏洞相对较少,但由于 Linux 系统在网络服务应用领域占有较高的比例,所以其安全漏洞存在的风险和威胁更为严重。例如,RHEL Linux 系统内核网络协议栈实现(net/ipv4/udp.c)中存在一个远程拒绝服务安全漏洞(CVE 2010 4161),攻击者通过向目标主机上任意开放的 UDP 端口发送一个特殊构造的 UDP 数据包,就可以发起对目标主机的 DoS 攻击。Linux 系统的每个网络服务都依赖于内核中的网络协议栈实现,一旦这些实现代码中存在具有远程代码执行危害后果的安全漏洞,不管 Linux 系统开放什么服务,都可能被攻击者用于实施远程渗透攻击。

LAMP(Linux/Apache/MySQL/PHP)是目前互联网上应用最为广泛的 Web 站点解决方案,即以 Linux 操作系统作为网站运行的服务器基础平台,以 Apache 提供的 HTTP/HTTPS 作为 Web 服务,以 MySQL 数据管理系统作为 Web 应用程序的后台数据库,以 PHP 语言作为 Web 应用程序的开发语言。在这种高效的 LAMP 组合中,一旦任何一个组件存在安全漏洞,都会被利用进行目标主机的远程渗透攻击。例如,早期 Apache mod

rewrite 模块中存在对 LDAP 协议 URL 处理过程中的溢出漏洞(CVE-2006-3747),可以对 Web 服务器通过 TCP 80 端口进行远程溢出攻击,从而获得 Web 服务器的本地访问权。又如,MySQL:sha256_password 认证长密码拒绝服务式攻击漏洞(CVE-2018-2696),该漏洞源于 MySQL sha256_password 认证插件,该插件没有对认证密码的长度进行限制,而直接传给 my_crypt_genhash(),用 SHA256 对密码加密求哈希值。该过程需要大量的 CPU 计算,如果传递一个很长的密码时,会导致 CPU 耗尽;还有,利用 PHP HTTP PROXY 环境变量安全漏洞(CVE-2016-5385)中 HTTP PROXY 环境变量未能过滤构造的客户端数据这一缺陷,远程攻击者通过构造 HTTP 请求的 Proxy 标头,可将 HTTP 数据流重定向到任意的代理服务器。除此之外,运行于 Linux 平台的 FTP、Samba、Sendmail 等服务对应的各类软件,都被发现存在不同程度的安全漏洞。

2. 针对远程渗透攻击的防范方法

由于远程渗透攻击的实现主要利用了被攻击目标主机存在的安全漏洞,所以加强安全漏洞的检测和修补是防范攻击的基础。

(1) 只开启需要的服务。网络远程渗透攻击中需要借助主机上开启的服务,即利用服务存在的漏洞实施攻击。开启服务需要同时启用服务进程,并打开对应的端口。对于互联网上的服务器来说,只需要开启与业务相关的最基本的网络服务,其他的应全部禁用。

(2) 使用安全性高的服务软件。互联网上的一个协议一般会同时对应多款服务软件,虽然每一款软件的基本功能都是基于相同的协议标准来开发的,但代表各自特点的扩展功能可能不尽相同。同时每一款软件的应用表现也不完全一致,有些软件注重操作的友好性却忽视了安全性,而有些软件有可能在强调安全性的同时使易操作性不尽如人意。例如, Linux 系统中可以分别通过 Apache、Nginx、Tomcat 来提供 HTTP 网络服务,这 3 款软件虽然都提供 Web 服务功能,但其应用特点不尽相同。其中,Apache 不但可跨平台运行(可运行于 UNIX、Linux 和 Windows 系统中),还具有较高的安全性,以及拥有快速、可靠、简单的 API 扩展,是互联网上使用最多的 Web 服务软件;Nginx 作为一款轻量级的网站服务软件,具有很好的稳定性和丰富的功能,且占用系统资源较少;Tomcat 属于轻量级的 Web 服务软件,一般用于开发和调试 JSP 代码,通常认为 Tomcat 是 Apache 的扩展程序。作为 Web 服务器,如果追求性能可以选择 Nginx,而如果强调安全性则选择 Apache。出于安全考虑,在应用功能能够满足需求的前提下,应尽可能选择安全性高的服务软件。

(3) 及时更新软件。及时更新软件可以增加软件自身的新功能,解决以前版本的漏洞或缺陷,增加软件的稳定性和对新的操作系统提供更好的支持等,尤其是对发现的软件安全漏洞需要进行及时修补。例如,在 RHEL、CentOS、Fedora Core 等 Red Hat 系列 Linux 发行版本中,可以通过“yum update”命令来将软件更新到最新版本,并通过“chkconfig level 3 yum on”命令来激活“/etc/cron.daily/yum.cron”,再通过 Crond 服务来配置系统的自动更新时间。需要注意的是,在进行软件版本升级前,需要对服务软件在新版本环境中进行测试,测试无误后再升级,因为在旧版本下运行良好的软件不一定会适应新版本的要求。

(4) 设置访问控制机制。Linux 系统在启动时需要开启一些系统服务,如何根据需要开启相应的服务,并禁用不需要的服务,不但可以有效地利用系统的资源,更有利于系统的安全。Linux 系统提供了一个被称为“超级守护进程”的 xinetd(eXtended InterNET Daemon)工具。在系统启动时由 xinetd 来负责统一管理需要启动的进程,在系统启动后,

当相应请求到来时需要通过 xinetd 的转接来唤醒被 xinetd 管理的进程。同时, xinetd 内建了基于远程主机地址、网段及域名的访问控制机制, 并支持分时间段的访问控制。另外, xinetd 还能够限制服务并发运行数、服务进程数和同一主机的最大网络连接数, 此功能可以有效地缓解对主机的 DoS 攻击。还有, xinetd 支持将网络服务绑定到指定的网络接口与监听端口上, 以降低被扫描和攻击的风险。除 xinetd 工具之外, Linux 系统集成的 netfilter/iptables 防火墙解决方案可以有效地加强对网络边界的安全管理。

3.3.3 DNS 服务器的攻防

DNS(Domain Name System, 域名系统)是互联网中绝大多数应用的实际寻址方式, 域名是互联网上的身份标识, 是不可重复的唯一标识资源。DNS 以其操作的便捷性在丰富了互联网应用的同时, 因其在互联网应用中的重要性, 已成为网络攻击的主要对象。

1. BIND 介绍

BIND(Berkeley Internet Name Domain)是互联网上使用最为广泛的域名解析软件, 目前有 90% 以上的域名服务器都使用 BIND 来解析。BIND 由加州大学伯克利分校开发, 目前有 BIND 8.x 和 BIND 9.x 这两个不同发展方向的版本, 其中 BIND 8.x 中融合了许多提高效率、增强稳定性和安全性的技术; 而 BIND 9.x 则增加了一些新的应用功能, 如支持 IPv6、提供公开密钥加密、支持多处理器、提供线程安全操作、提供增量区传送等。从 BIND 9.x 开始支持 View 功能, 利用 BIND 9.x 中的 View, 在具体配置中通过 View 与 ACL 的协同工作, 以实现根据用户源 IP 地址智能解析对应服务器的 IP 地址的功能。如果要使同一个域名指向不同的 3 个网域, 只需要在 named.conf 文件中通过 ACL 定义 3 个不同的网域, 即 View 分别指向同一个域名的 3 个不同的网域, 之后当处于不同 View 中的用户访问这个域名时, 将通过 BIND 解析到不同网域对应的 IP 地址, 从而实现了 DNS 的智能解析功能。BIND 9.x 的最新版本可在 <http://www.isc.org> 中下载使用。

BIND 通过对区文件(zone file)的管理实现对 DDNS(Dynamic Domain Name Server, 动态域名服务)的域名授权和查询, BIND 的组成结构如图 3-7 所示。其中, named 进程是 BIND 服务器的核心, named 启动时读取初始化文件 named.conf 并配置数据文件。当 DNS 客户端的解析器发出 DNS 解析请求时, 由 named 进程将查询结果(即域名对应的 IP 地址)发送给客户端。named.conf 把所有区文件绑定在一起, 以便 named 进程可以根据域名查询要求通过 named.conf 中的记录来读取区文件。作为网络应用中的关键服务, named 进程在工作过程中也会根据 BIND 的配置提供日志记录。

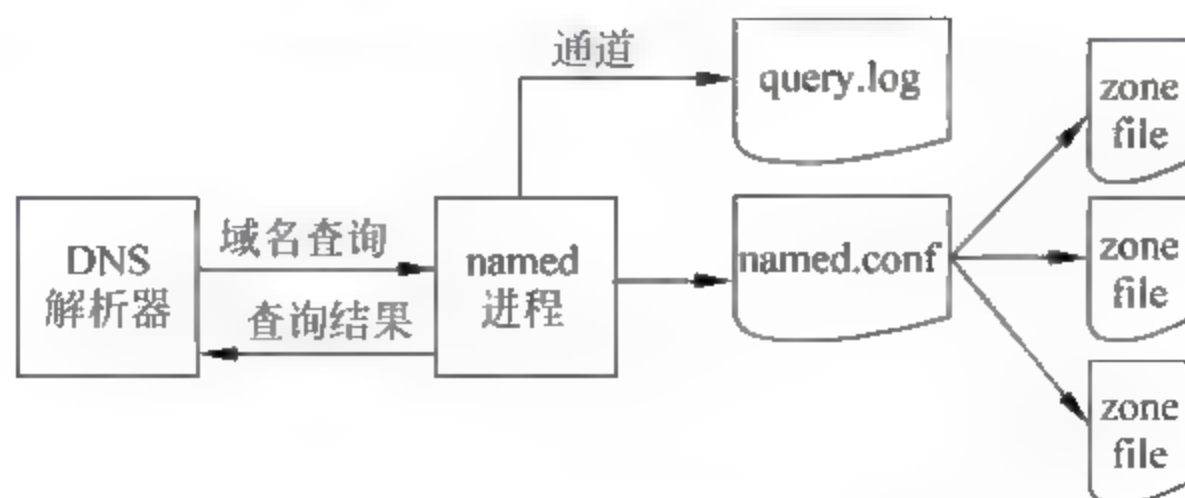


图 3-7 BIND 的组成结构

2. 一个典型的 DNS 攻击过程分析

2009 年 5 月 19 日晚,受暴风影音软件存在的设计缺陷及免费智能 DNS 软件 DNSPod 的不健壮性影响,黑客通过僵尸网络控制下的 DDoS 攻击,致使我国江苏、安徽、广西、海南、甘肃、浙江等省在内的 23 个省出现罕见的断网故障,即“5·19 断网事件”。这一事件告诫人们:在互联网中,越是由基础服务产生的安全威胁,影响力越大,范围越广。作为互联网基础服务的 DNS,每天有海量的域名解析信息产生,其个体的安全性已经直接影响着互联网的安全。与此同时,随着网络应用的不断复杂化,当潜在的条条安全暗流通过某种规则汇集在一起时,所形成的巨浪足以使正常的网络运行秩序产生混乱直至瘫痪。“5·19 断网事件”再次引起了人们对 DNS 服务及其相关安全威胁的关注。在这一事件中,僵尸网络控制下的 DDoS 攻击是问题产生的根源,免费软件的后门是问题产生的诱因,DNS 服务的脆弱性是问题产生的关键,而 DDoS 攻击、软件后门及 DNS 服务之间的内在关联是这一事件得以发生的潜在因素。

“5·19 断网事件”是多种综合因素产生的结果,其攻击过程示意图如图 3-8 所示,具体实现步骤如下。

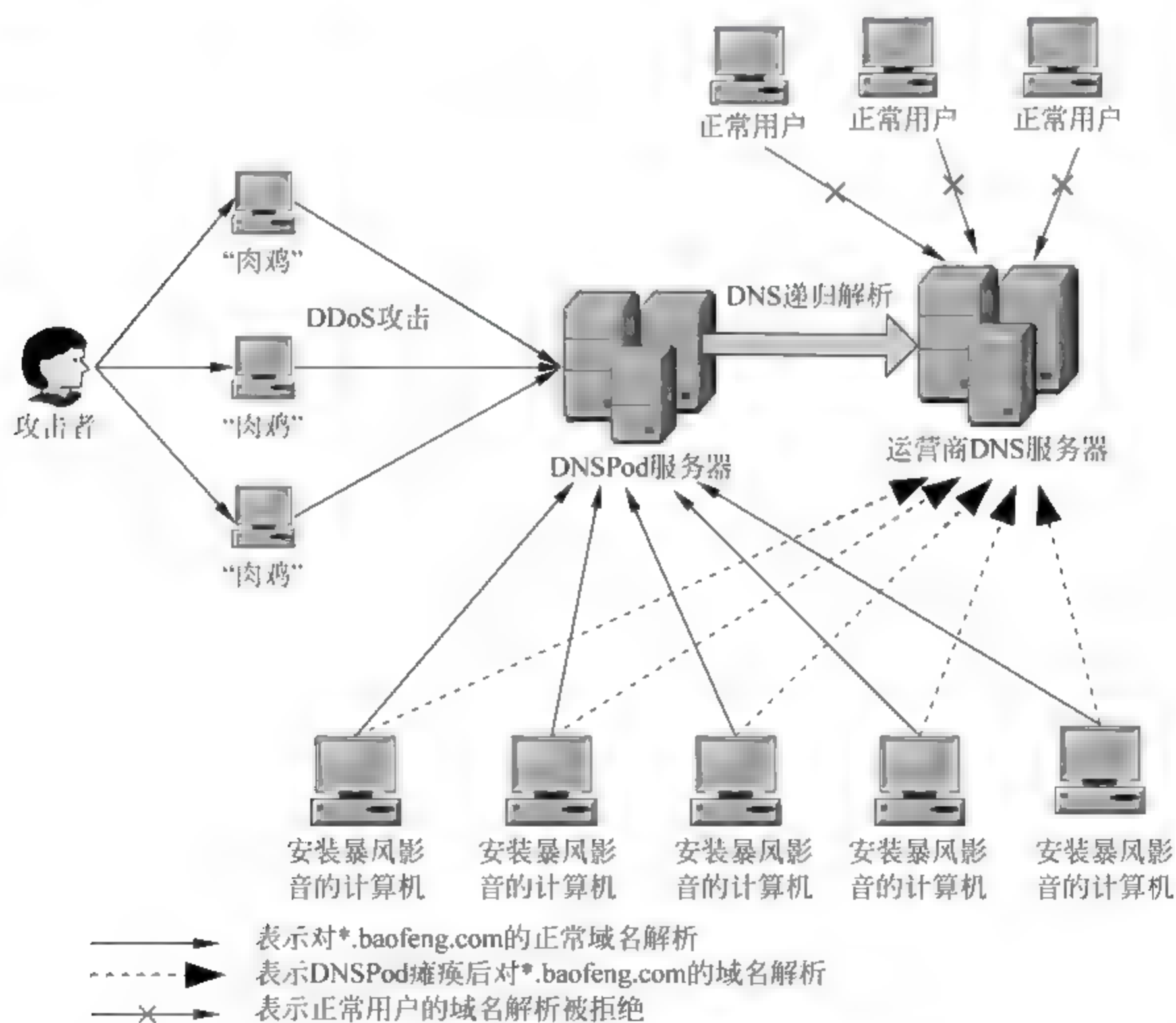


图 3-8 “5·19 断网事件”攻击过程示意图

① 攻击者(黑客)通过控制互联网上大量的“肉鸡”(被僵尸网络控制的计算机)向免费动态 DNS 服务器 DNSPod 发起 DDoS 攻击,使 DNSPod 服务器无法为正常用户提供域名解析服务,直至瘫痪。

② 因为暴风影音网站(*.baofeng.com)的域名解析使用的是 DNSPod 服务器,当

在大范围推广时存在一定的难度。可喜的是：目前 ICANA 已经在部分根域系统（如 .org）上部署了 DNSSEC，以提高根域服务器的安全性，此举说明 DNSSEC 已从理论探讨和区域性试验开始走上实际应用了。

（6）DDoS 攻击的防范。近年来，采用 DDoS 对 DNS 服务器的攻击不断出现。对于采用树形结构的 DNS 体系，域名节点越是靠近根，所受到的 DDoS 攻击威胁也就越严重。解决 DDoS 攻击的最有效方法有以下 4 种：一是部署 IDS（Intrusion Detection Systems，入侵检测系统），从单一技术和设备来看，IDS 是目前防范 DDoS 攻击最有效的方法；二是对于重要的 DNS 服务器，可分别在不同的 IDC 中部署，通过冗余方式来提高 DNS 的安全；三是在防火墙上通过设置策略，对于超过某一限定值的 DNS 请求报文进行过滤；四是通过管理软件，对排名靠前的 DNS 解析请求报文进行分析，重点分析那些流量在短时间内急剧增大的报文，对可疑报文进行过滤处理。

4. 针对基于 BIND 软件的 DNS 的安全管理方法

虽然 BIND 对 DNS 提供了大量的安全防范，但是如果配置不当或没有进行必要的安全设置，其安全性仍然无法得到体现。下面结合 Linux 系统中对 BIND 软件的配置，介绍常见的安全管理方法。

（1）正确地配置 DNS 服务器。在 Linux 系统中，DNS 服务由 named 守护进程进行控制，该进程从主文件“/etc/named.conf”中获取具体的配置信息。除此之外，还有许多与之相关的配置文件，如根域名配置服务器指向文件“/var/named/named.ca”、用户配置区正向解析文件“/var/named/name2ip.conf”、Localhost 区正向域名解析文件“/var/named/localhost.zone”等。Linux 系统中基于 BIND 软件的 DNS 配置是由一组文件组成的，在具体配置过程中不但要清楚不同文件的功能及存放位置，而且要掌握不同文件的配置方法，同时还要熟悉不同配置文件之间的关系。一旦一个配置存在缺陷，将会留下安全漏洞。在安装 BIND 软件包时，系统自动安装了用于对 DNS 配置文件进行检查的工具，如 nslookup、dig、named-checkzone、host、named-checkconf 等，熟悉这些工具的功能及应用，对检查 DNS 配置的正确性、防止出现安全漏洞是很有帮助的。

（2）隐藏 BIND 的版本号。对目标主机的操作系统类型及版本号等信息进行搜集是网络攻击前需要完成的一项工作内容，只有掌握了目标主机的详细信息，才能从中发现可利用的漏洞。一般情况下，通用软件的设计缺陷是与特定的版本相关的，所以版本号的搜集对攻击者来说是十分关键的。攻击者可以利用 dig 命令查看 BIND 软件版本号，进而知道该版本的 BIND 软件存在哪些漏洞。为此，隐藏 BIND 的版本号是很有必要的，具体可在配置文件“/etc/named.conf”的 option 部分添加 version 声明，将系统默认显示的版本号覆盖掉。例如，可通过以下配置，当利用 dig 查看版本号时，显示为：“The platform does not provide version queries”。

```
options {  
    version "The platform does not provide version queries"  
}
```

同时，在 DNS 配置文件避免使用 HINFO 和 TXT 资源记录，可以使攻击者无法得到 DNS 服务器的相关信息。

(3) 控制区域(zone)传输。DNS 区域传输(zone transfer)是指备用服务器通过主服务器的数据来更新自己的区域(zone)数据库。出于服务的可靠性考虑,一般不会仅提供一台 DNS 服务器,而是通过设置主/从(master/slave)DNS 服务器来实现安全备份功能。当设置了主、从备份服务器后,从服务器需要从主服务器中读取并更新自己的区域数据库,这便是 DNS 的区域传输操作。区域传输的主要对象是区域数据库,该数据库保存着网络架构中的主机名、主机 IP 地址列表、路由器名、路由 IP 列表,以及各主机所在位置和硬件配置等重要信息。

在 BIND 的默认配置中,区域传输是全部开放的,即 DNS 服务器允许对任何主机进行区域传输操作。如果攻击者假冒备用 DNS 服务器,向指定主 DNS 服务器(攻击主机)请求进行区域传输,就会收集到该 DNS 服务器所在网络架构中的所有配置信息。为了加强对 DNS 服务器的安全保护,需要严格限制允许区域传输的主机,一般一个主 DNS 服务器只允许它的从 DNS 服务器执行区域传输操作。对于 BIND 软件,可以通过如下的 allow-transfer 命令来控制。

```
acl"zone-transfer"{172.16.1.0;172.16.1.254}
zone"yourdomain.cn"{
type master;
file"yourdomain.cn";
allow-transfer {zone-transfer;};};
```

这样,只有 IP 地址在 172.16.1.0 至 172.16.1.254 范围内的主机才能够同 DNS 服务器进行区域传输操作,限制了其他主机的操作。

(4) 限制反向解析请求。在 DNS 系统中,一个 IP 地址可以对应多个域名,即多个域名可以同时指向同一个 IP 地址。因此,由 IP 地址来查询域名,理论上是可行的,但实际上是不现实的,因为这种查询操作会遍历整个域名树,这在 Internet 上是不现实的。为了避免类似操作的发生,DNS 提供了一个被称为“反向解析域”(in addr. arpa)的区域,由该区域负责向需要从 IP 查询域名的请求提供应答服务。例如,一个 IP 地址为 210.98.95.2 的反向解析域名表示为 2.95.98.210.in addr. arpa,反向解析域名与 IP 地址正好相反,同时在后面加上了“.in addr. arpa”。因为域名结构是自底向上(从子域到根域),而 IP 地址结构是自顶向下(从网络到主机)的。实质上反向域名解析是将 IP 地址表达成一个域名,以地址作为索引的域名空间。

如果任何用户都可以向 DNS 服务器发送反向解析请求报文,这无异于给 DNS 服务器实施 DoS 攻击提供帮助。所以,需要限制 DNS 服务器的反向解析服务,只允许特定 IP 地址范围内的主机使用该服务。例如,通过以下设置,只允许 IP 地址在 172.16.1.0 网段的主机使用该 DNS 服务器提供的反向地址解析服务。

```
options{
allow-query {172.16.1.0/24};
};
zone "yourdomain.cn";
type master;
```

```
file "yourdomain.cn";
all-query{any;};
};
zone "1.16.172.in-addr.arpa" {
type master;
file "db.172.16.1";
allow-query {any;};
```

限制反向解析服务的范围,除能够有效保护 DNS 服务器外,还可以拒绝接收所有没有注册域名的 IP 地址发来的邮件。目前,多数垃圾邮件发送者使用动态分配或者没有注册域名的 IP 地址来发送垃圾邮件,以逃避追踪。因此,在邮件服务器上拒绝接收来自没有域名的 IP 地址发来的邮件可以大大降低垃圾邮件的数量。

3.3.4 Apache 服务器的攻防

Windows 和 Android 分别在桌面操作系统和移动智能终端领域的广泛应用,使得它们成为攻击者的主要选择目标。此现象充分说明攻击者只会选择有利用价值的目标对象,而使用越广泛的系统才潜藏着可被利用的价值。同样,在 Web 服务器应用中,Apache 的大量部署,使其成为攻击者在互联网 Web 应用领域的主要研究对象和攻击目标。

1. 针对 Apache 服务器常见攻击方式

攻击者选择 Apache 服务器,主要借助 Apache 软件自身存在的安全漏洞和错误的配置,同时还利用了传统的 DoS、缓冲区溢出等方式攻击,借助 HTTP/HTTPS 协议设计上的不严谨性实现攻击行为。

(1) 泛洪攻击。泛洪(flood)攻击是一种中断网络服务的常见攻击方法,通常通过发起 ICMP(Internet Control Message Protocol, Internet 控制报文协议)包或 UDP(User Datagram Protocol, 用户数据报协议)包实施具体的攻击行为。通过向目标主机发送泛洪数据包,使目标主机或连接主机的网络负载过重,进而无法提供正常的网络服务。要实施泛洪攻击,攻击者的网络带宽一定要大于被攻击主机所使用的网络带宽。

使用 UDP 数据包进行攻击是利用了 UDP 协议的工作原理。当攻击者发送了 UDP 数据包后不会有任何数据包返回到攻击者的主机,这种基于单向数据流的工作机制很适合攻击者通过向目标主机发送大量的数据包来迫使其无法提供正常的服务。使用 ICMP 数据包进行攻击是利用了该协议可以根据不同的应用需求来构造不同的数据包这一特点,攻击者通过构造有缺陷的数据包来扰乱正常的网络工作机制。泛洪攻击的本质是攻击者通过欺骗目标主机,让其相信所接收到的数据包都是正常的。

(2) 硬盘攻击。不论是机械硬盘还是固态硬盘,其总体结构都是相似的。硬盘主要由处理器、缓存、Boot ROM 和主存储介质等几部分构成,对于机械硬盘还有电机驱动电路和磁头控制电路等部件。由于硬盘的电路板上已经具有了 CPU、内存和 ROM,所以可以将硬盘看作是一个小型的计算机系统,在固件的控制下独立运行。硬盘通电时,处理器执行片段内的 Loader 代码,这部分代码会加载 Boot ROM 到缓存中并执行。Boot ROM 得到控制权后,会依次初始化基本外设,初始化主存储介质,从主存储介质上加载固件主体,启动 IDE/SATA 总线接口驱动模块,并进入待命状态,此时计算机即可对硬盘进行操作。

体方法是修改 Apache 的配置文件“/etc/httpd.conf”，在找到“ServerSignature”和“ServerTokens”关键字后，将其设定为“ServerSignature Off”和“ServerTokens Prod”，然后重启 Apache 服务器。

(2) 创建安全目录结构。Apache 服务器包括多个目录，表 3-2 列出了其主要目录的功能及安全配置建议。

表 3-2 Apache 服务器主要目录的功能及安全配置建议

目 录 名	功 能	安全配置建议
ServerRoot	保存 Apache 的配置文件、二进制文件和其他服务器配置文件	只能由 root 用户访问
DocumentRoot	保存 Web 站点的内容，包括 HTML 文件和图片等	只能由管理 Web 站点内容的用户和使用 Apache 服务器的 Apache 用户和 Apache 组访问
ScriptAlias	保存 CGI 脚本	只能被 CGI 开发人员和 Apache 用户访问
Customlog	保存访问日志	只能由 root 用户访问
Errorlog	保存错误日志	只能由 root 用户访问

(3) 为 Apache 分配专门的执行账户。为避免因使用 root 作为 Apache 的执行账户带来的安全问题，一般在对 Apache 配置结束后需要分配一个专用的执行账户，不再使用 root。Apache 账户权限的分配遵循“最小特权原则”，即要求该账户对系统及数据进行访问时只拥有必须的最小权限。保证用户能够完成所操作的任务，同时也确保将非法用户或异常操作所造成的损失降到最小。

(4) Web 目录的访问控制。在 Web 服务器中，将需要发布的 Web 站点的文件保存在 Web 目录中，需要确保其安全，防止非授权访问和非法篡改。

Apache 服务器在接收到用户对一目录的访问请求时，会查找 DirectoryIndex 指令指定的目录索引文件，默认情况下该文件为 index.html。如果该文件不存在，那么 Apache 会通过创建一个动态列表为用户显示该目录的内容。通常这样的配置会暴露 Web 站点的结构，因此需要修改配置“/etc/httpd/conf/httpd.conf”，搜索“Options Indexes FollowSymLinks”，修改为“Options Indexes FollowSymLinks”即可。其中，在“Options Indexes FollowSymLinks”的“Indexes”前面加上“-”符号表示禁止目录索引，如果是“+”符号则表示允许目录索引，“FollowSymLinks”表示允许使用符号链接。

(5) 利用.htaccess 加强对 Apache 服务器的安全管理。。htaccess 是 Apache 服务器上的一个基于文本的分布式配置文件，它提供了针对目录改变的配置方法，即将包含一些操作系统的.htaccess 文件保存在某一特定目录后，该目录及其下的所有子目录都会受到该文件的影响(index.html 文件除外)。。htaccess 通过自行修改其文件内容来实现权限控制，主要应用于为网页访问设置密码、自定义错误页面、改变首页的文件名(如 index.html)、禁止读取文件名、重定向文件等。下面通过几个实例来说明.htaccess 文件的配置和应用。

① 自定义错误页面。当用户访问某一网站时，不合理的访问或网站自身存在问题时，会出现不同的错误返回页面。攻击者可以通过该错误返回页面中的信息来了解 Apache 服务器的有关配置情况，并以此作为某种判断的依据。可以借助.htaccess 来控制对错误返回

页面信息的显示内容。HTTP 协议的错误代码被标准化定义为 400~505,但通过对 .htaccess 的配置,可以使 Web 服务器处理错误时能够进行个性化的定制,而不是被协议标准化的默认页面。配置错误页面的重定向语法如下。

```
ErrorDocument [error code][url]
```

其中,“error code”为错误代码;“url”为指定保存自定义错误信息的页面所在的地址。例如,如果在当前目录下有一个保存自定义错误信息的页面文件 payattention.html,使用它作为 404 错误页面,可以写为:

```
ErrorDocument 404/payattention.html
```

404 错误页面是客户端在浏览网页时,服务器无法正常提供信息,或者服务器无法回应且不知道原因所返回的页面,而利用 .htaccess 文件则可以对其进行任意的修改。具体操作时,只需要将 payattention.html 和 .htaccess 两个文件同时上传到指定的目录中即可。

② 网站目录的密码保护。要使用 .htaccess 进行 Web 站点所在目录的密码保护,可通过两个步骤来实现:配置 .htaccess 文件和创建 .htpasswd 密码文件。.htaccess 文件的相关内容如下。

```
AuthName "Section Name"  
AuthType Basic  
AuthUserFile /full/path/to/.htpasswd  
Require valid-user
```

其中,“Section Name”将出现在用户端弹出页面的密码输入框中,可以自行定义;“/full/path/to/.htpasswd”是密码文件 .htpasswd 的绝对路径。密码文件 .htpasswd 的内容格式为“username:password”;“Require valid user”表示 .htpasswd 文件中设置的任何一个合法用户都可以访问。

通过以上的设置,当用户试图访问被 .htaccess 文件密码保护的目录时,浏览器会弹出要求输入账户名和密码的对话框,只有当正确输入后才能够访问。

③ 限制来访主要的 IP 地址范围。对于只需要对特定人群(特定 IP 地址范围)开放的 Web 站点,可在 .htaccess 中对指定 IP 进行限制,有效防止其他用户访问该站点。例如:

```
Order deny, allow  
deny from all  
allow from 172.16
```

通过以上设置,表示只允许 172.16.0.0 网段的用户访问该站点,其他用户都将被拒绝。

通过上述的几个实例可以看出,使用 .htaccess 来保护网站更为安全和方便。因为利用 .htaccess 实现密码保护,可以有效地抵御字典攻击和暴力破解。

3.4 Linux 用户提权方法

通过远程渗透技术,攻击者可以获得系统的远程访问权限,并能够实现远程登录。在完成了远程登录后,攻击者就转向对本地主机的攻击。本地主机攻击过程中最重要的是用户权限的提升。

3.4.1 通过获取“/etc/shadow”文件的信息来提权

Linux 系统的账户分为特权账户 root、普通用户账户和系统用户账户三大类,并采用 VFS(Virtual File System,虚拟文件管理)来控制每个用户对文件的访问。出于安全考虑,在一些 Linux 发行版本中用特别分配的系统用户账户来启动和运行网络服务,只有一些频繁访问系统资源的特殊网络服务(如 Samba)才直接使用 root 账户权限运行。

需要特别说明的是,为了养成安全使用 Linux 系统的习惯,建议系统管理员使用普通用户账户来登录和操作 Linux 系统,只有确实需要使用 root 权限来配置和管理系统时,再通过 su、su -或 sudo 命令将权限提升到 root 用户账户。对于普通用户账户,坚持最小权限分配原则,一般禁用 root 账户权限。

通过获取“/etc/shadow”文件的内容来对本地用户进行权限提升,主要分为获取“/etc/shadow”文件和破解“/etc/shadow”文件以获得用户密码两个过程。

1. 获取“/etc/shadow”文件

通过远程渗透方法,攻击者如果获得了 root 账户的登录密码且系统允许 root 账户远程登录,那就可以直接登录系统进行任意的操作。但是,由于 root 账户的重要性,大部分情况下其登录密码是很难获得的,攻击者一般得到的是普通用户账户的登录权限。普通用户账户对系统的操作是受限的,一般很难完成预定的操作,这时就需要通过提权技术,将普通用户账户的权限提升到 root 权限。

在早期的 Linux 版本中,包括 root 在内的所有账户信息(包括用户名和对应的密码)全部保存在“/etc/passwd”文件中,并且普通用户也可以读取该文件的内容。当 Linux 系统引入了“the Shadow Suit”组件后,将用户账户的密码加密后单独存放在“/etc/shadow”文件中,而且只有 root 用户才能够读取该文件中的信息。

如何才能得到 shadow 文件的内容呢?首先要能够得到 shadow 文件,然后再对 shadow 文件进行破解。因为只有具有 root 权限的用户才能够读取 shadow 文件,在无法直接获得 root 权限用户账户信息的前提下,可借助一些以 root 权限运行的服务中存在的文件任意读写漏洞来间接获得。当具有 root 权限运行的程序中存在代码任意执行安全漏洞时,可以代替攻击者主动打开具有 root 权限的 shell 命令行连接,有了该连接就可以读取“/etc/shadow”文件。攻击者在获得了 shadow 文件后再通过破解其密码以获取 root 用户的密码。

2. 破解“/etc/shadow”文件

用户密码破解是网络攻击中的一个最基本的操作,然而由于系统的复杂性和多样性,这

不管是运行在内核态的代码,还是运行在用户态的应用程序,以及位于用户态的进程向内核的调用,甚至是程序在运行过程中从用户态向内核态的切换,都会存在程序漏洞或操作机制上的安全隐患。尤其是 Linux 的内核代码,因其具有开源性,便成为攻击者研究的主要对象。一旦发现内核代码中存在高危提权漏洞,攻击者便可以方便地对用户进行提权操作,并实现对大量主机系统的操作,其利用价值和产生的威胁是可想而知的。

2016 年 1 月, Linux 系统被发现在内核中存在一个高危级别的本地提权 0day 漏洞(编号为: CVE-2016-0728),该漏洞属于 Linux 平台上的 UAF(Use After Free)漏洞。其中, UAF 漏洞产生根源是迷途指针(dangling pointer),已分配的内存释放之后,其指针并没有因为内存释放而变为 NULL,而是继续指向已释放内存。如果是良性迷途指针,该指针不会再被使用;而如果是恶性迷途指针,则该指针还会被用来对已释放内存进行读写操作。CVE-2016-0728 漏洞的产生,主要是由于 keyrings 组件中的引用计数问题。keyrings 的主要功能是为驱动程序在内核中保留或缓存安全数据、身份认证密钥、加密密钥及其他数据。它使用一个 32 位的无符号整数做引用计数,但是在计数器出现溢出的时候没有进行合理的处理。当对象的引用计数达到最大时会变成 NULL,因此释放对象的内存空间。而此时程序还保留对引用对象的引用,所以形成了 UAF 漏洞,可实现对本地用户的提权操作。该漏洞影响 Linux 内核 3.8 及以前版本,已影响到大量的 Linux 个人计算机、服务器及大量安卓设备(包括智能手机和平板电脑)。

3.4.3 针对本地提权攻击的安全防御方法

针对本地提权攻击,最有效的安全防范方法依然是及时更新系统的补丁程序,以便在第一时间修补存在的安全漏洞。除此之外,结合本节介绍的几类提权攻击方法,下面主要基于 Linux 服务器的应用,从系统管理的角度提些建议。

针对 SUID 特权程序,管理员首先要清楚 Linux 系统在默认安装时,哪些系统程序使用了 SUID 特权位设置,程序如果不需要就尽可能将其禁用。对于在 Linux 系统上运行的应用程序,管理员必须知道是否会启用 SUID 特权位设置,并评估可能存在的安全风险。对于安全风险大的 SUID 特权程序,应尽可能去除 SUID 特权位的设置,如果确实要使用,必须实时关注其安全状况。即使是安全风险小的 SUID 特权程序,管理员也要做到“清单式”管理,即对使用的 SUID 特权程序建立应用清单,及时安装安全补丁程序。

针对利用代码漏洞进行本地提权的问题,最根本的解决办法还是及时升级操作系统并安装补丁程序,同时辅助以必要的安全配置。例如,禁止 root 用户进行远程登录、对特权用户设置强口令、使用 SSH 对服务器进行远程管理等。

另外,针对 Linux 在访问控制机制中存在的本地提权漏洞,可使用 SELinux 安全增强模块来提高 Linux 抵御本地攻击的能力。早期的 Linux 采用自主访问控制(Discretionary Access Control, DAC)来保证系统的安全性,根据用户标识和所有者权限来确定是否允许访问。这种机制的缺陷是忽略了用户的角色、数据的敏感性和完整性、程序的功能和可信性等安全信息,因此不能提供足够的安全性保证。而 Linux 在 2.6 内核之后集成了 SELinux 组件,在该组件中引入了强制访问控制(Mandatory Access Control, MAC)机制,可以有效地解决早期 Linux 系统中存在的一些问题。MAC 根据用户操作对象(如普通文件、目录、设备、端口、被调用的进程等)所含信息的敏感性,以及用户操作(如读、写、执行等)在访问这

些信息时的安全授权来限制对用户操作对象的访问。SELinux 是一种通用的、灵活的、细粒度的 MAC 机制,为用户操作和用户操作对象定义了多种安全策略,能够最大限度地限制进程的权限,保护进程和数据的安全性、完整性和机密性,从而解决了 DAC 的脆弱性和传统 MAC 的不灵活性等问题。

习 题

1. 简述 Linux 系统的安全机制及主要实现方法。
2. 分析 PAM 技术的实现过程,并介绍其应用特点。
3. 分析 Linux 的权限分配特点及访问控制机制的实现方法。
4. Linux 环境中的用户账户分为哪几类? 如何获取其信息? 如何进行安全防范?
5. 结合安全漏洞的概念,分析漏洞在网络远程渗透攻击过程中发挥的功能,以及如何
进行安全防范?
6. 以本文介绍的“5·19 断网事件”为例,详细分析 DNS 服务器存在的安全隐患及攻击
的实现过程。在此基础上,结合 Linux 环境下 BIND 软件的配置方法,介绍 DNS 服务器的
安全防范措施。
7. 结合实际部署的 Apache Web 服务器,通过具体的操作,分析其存在的主要安全缺
陷及其可能产生的结果,并介绍其安全防范方法。
8. 简述分块编码远程溢出的原理及实现方法。
9. 通过实际操作,掌握利用 htaccess 对 Apache 服务器进行安全保护的方法。
10. 介绍 Linux 系统中对普通用户账户进行提权的方法。
11. 通过实际操作,在掌握 SUID 特殊权限位功能及设置方法的基础上,以 Linux 系统
中的 passwd 程序为例来说明 SUID 特殊权限的实现过程和应用特点。

第4章 恶意代码的攻防

恶意代码(Unwanted Code、Malicious Code 或 Malware)是指未经授权认证,攻击者从其他计算机系统经存储介质或网络传播,以破坏计算机系统完整性为目标的一组指令集。该指令集并非全部是二进制执行文件,还包括脚本语言代码、宏代码或寄生于其他代码中的一段指令等。恶意代码由攻击者根据个人意图而编写,其目的包括窃取他人计算机上的信息、远程控制被攻击的计算机、占用他人计算机或网络资源、拒绝服务、进行破坏、炫耀个人技术或恶作剧等。恶意代码包括计算机病毒、蠕虫、木马、后门、僵尸网络等。恶意代码攻击是所有网络攻击行为中涉及面最广、影响力最大、自动化程度最高的一种攻击方式。涉及面广是指目前恶意代码攻击的对象几乎涉及采用不同结构、不同应用功能、不同通信方式的所有智能设备,以及能够运行程序代码的微系统;影响力大是指一个恶意代码一旦出现,将会借助互联网快速传播,有些恶意代码还会在传播过程中不断演变,以适应环境的变化;自动化程度高是指恶意代码的攻击过程实现了自动化、模块化和智能化,以便能够在更短时间内攻击更多的目标。本章重点从攻击原理和行为分析两个方面介绍恶意代码的攻防技术。

4.1 计算机病毒

计算机病毒是最早出现的恶意代码,也是蠕虫、木马等恶意代码产生的基础,所以较为系统地了解计算机病毒的概念和机制对全面学习恶意代码具有重要意义。

4.1.1 计算机病毒的起源

1949年,计算机之父约翰·冯·诺依曼(John von Neumann)在《复杂自动机组织》一书中提出了计算机程序能够在内存中自我复制的概念,这为计算机病毒的产生打下了基础。

1960年,美国人约翰·康维编写了“生命游戏”(Conway's Game of Life)程序。程序运行时屏幕上会出现许多运动变化着的表示“生命元素”的图案,元素在过于拥挤和稀疏时都会因缺少生存条件而死亡,只有处于合适环境中的元素才能自我复制并进行传播,这被称为游戏编程的起源,也是计算机病毒自我复制特征的体现。

1966年前后,来自美国贝尔实验室的3位年轻程序员——道格拉斯·麦基尔罗伊(H. Douglas McIlroy)、维克多·维索特斯克(Victor Vysotsky)及后来的美国国家安全局(NSA)的首席科学家罗伯特·莫里斯(Robert H. Morris)共同开发了一个被命名为“达尔文”(Darwin)的游戏环境。游戏规则是:参与游戏的双方各自编制能够自我复制并可保存在磁芯片(core)存储器中的程序,通过覆盖对手的程序与复制自身将对手程序“杀死”,即宣告胜利。该游戏就是著名的“磁芯大战”(Core War)。用于磁芯大战的游戏有多种,如有一个名为“爬行者”的程序(Creeper),每一次执行都会自动生成一个副本,很快计算机中的原有资料就会被这些爬行者侵蚀掉;还有一个名为“侏儒”(Dwarf)的程序在记忆系统中执行,

每到第5个“地址”(address)便会把那里所储存的资料删除,这会严重破坏原本的程序。磁芯大战游戏程序不但体现了计算机病毒在运行过程中的自我复制和攻击对方的特点,而且实现了多个程序员为了同一个目标而贡献各自的智慧。

1983年11月,美国计算机安全学家弗雷德·科恩博士研制出一种在运行过程中可以复制自身的破坏性程序,并将其命名为“Computer Virus”(计算机病毒)。专家们在VAX11/750计算机系统中运行此程序,至此,第一个病毒实验成功。

1986年年初,在巴基斯坦的拉合尔·巴锡特和阿姆杰德两兄弟编写了Pakistan病毒,即Brain(大脑)病毒,此病毒在一年内流传到世界各地。这是世界上第一例传播的病毒。1987年10月,Brain病毒在美国被发现,此后,世界各地的计算机用户也相继发现了形形色色的计算机病毒,计算机病毒一经出现,便以极其迅猛的速度增长。

4.1.2 计算机病毒的概念

作为一个计算机安全领域被大家熟知的名词,计算机病毒的概念从一提出就随着计算机技术的发展和人们对安全认识的不断加深而动态变化。不同的定义有着不同的侧重点,所以较为全面地了解不同定义的内涵,对深入学习计算机病毒的特征和机制有很大帮助。

1983年11月,计算机病毒之父弗雷德·科恩博士把计算机病毒定义为:“计算机病毒是一种计算机程序,它通过修改其他程序把自身或其演化体插入它们中,从而感染它们。”并于1988年著文强调:“计算机病毒不是利用操作系统的错误或缺陷的程序。它是正常的用户程序,它仅使用那些每天都使用的正常操作。”

汉堡大学(University Hamburg)计算机病毒测试中心的Vesselin Bontchev认为:计算机病毒是一种自我复制程序,它通过修改其他程序或它们的环境来“感染”它们,使得一旦调用“被感染”的程序就意味着调用“病毒”的演化体,在多数情况下,意味着调用与“病毒”功能相似的复制。

1994年2月18日,《中华人民共和国计算机信息系统安全保护条例》第二十八条给计算机病毒的定义是:“计算机病毒是指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据,影响计算机使用,并能自我复制的一组计算机指令或者程序代码。”

目前,大部分信息安全研究者认为:计算机病毒是一种程序,它用修改其他程序或与其他程序有关信息的方法,将自身的精确复制器或可能演化的复制器放入或链入其他程序,从而感染其他程序。

由于计算机病毒与医学上的“生物病毒”有着相似的破坏性和传染性特征,后来把这种能够自我复制且具备破坏功能的计算机程序称为计算机病毒。计算机病毒修改宿主程序,并将自身的精确复制或其演化的复制插入其中,从而感染该宿主程序。由于这种感染特性,病毒可随信息流的扩散而传播,从而破坏信息的完整性。

计算机病毒与生物病毒是两个不同范畴的概念。前者是人工制造,后者是自然产物;前者是机器编码,后者是核酸编码;前者是物理存储指令,后者以化学存储方式为主。尽管如此,二者在功能上及危害和感染的本质上是一致的。计算机病毒几乎具有生物病毒全部的生物学特征。从这个意义上来说,计算机病毒是一种可能的人工生命体(即人工病毒),其生命周期可以分为新病毒的产生、病毒传播及潜伏、病毒触发运行及破坏和病毒被反病毒程序查杀,如图4-1所示。从图4-1中可以看出,病毒变种一般产生于病毒传播、潜伏过程中,

同时计算机病毒具有自我繁殖、自我构造、自我进化等生命特征。

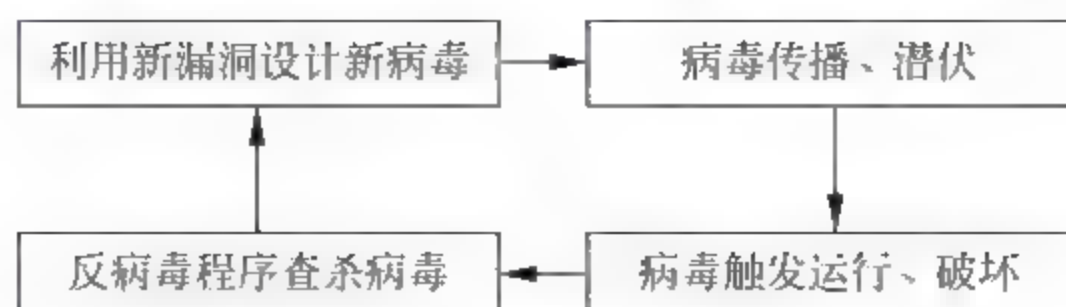


图 4-1 计算机病毒的生命周期

基于计算机病毒的算法特征和生命特征,病毒变种或未知病毒一般诞生于已知病毒的演化之中。病毒编写者在制造新病毒时,通常采用如下方式。

- (1) 对已知病毒进行编码分析。
- (2) 提取病毒的各种模块。
- (3) 运用不同的算法对已知病毒的模块进行组合,得到新的病毒。

4.1.3 计算机病毒的基本特征

TCP/IP 体系的开放性、计算机程序的自我复制性、计算机网络的共享性及计算机软硬件系统设计上的漏洞,为计算机病毒的产生与发展提供了物质基础,也决定了计算机病毒的结构。计算机病毒的这种结构也是其充分利用系统资源进行破坏活动的最合理体现。如图 4 2 所示,计算机病毒一般由感染标记、初始化模块、感染模块和表现模块组成。概括地讲,计算机病毒具有以下基本特征。

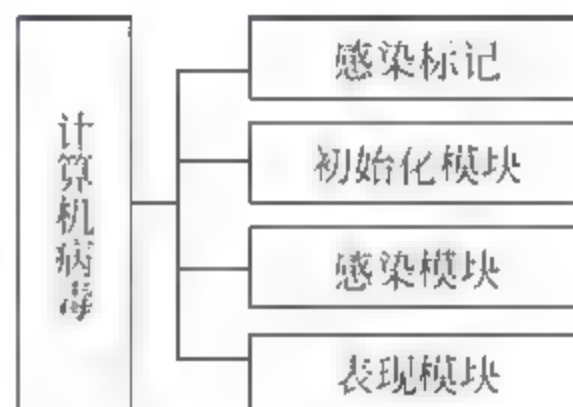


图 4-2 计算机病毒的结构

1. 破坏性

只有少部分计算机病毒的编写者是为了炫耀自己的技术,其病毒特征仅仅会影响计算机的正常运行,或者改变用户使用计算机的习惯;大部分计算机病毒都具有破坏性。所谓破坏性,是指计算机病毒在触发后会执行一定的破坏行为来达到病毒编写者的目的,即破坏文件或数据,具体表现为删除文件、格式化磁盘、占用网络带宽,甚至是破坏硬件。

2. 传染性

传染性是指计算机病毒能够把自己复制到其他程序的特性。传染性是计算机病毒最重要的特征,是判断一段程序代码是否为计算机病毒的依据。运行被计算机病毒感染的程序后,该带毒程序可以很快地感染其他程序,使计算机病毒从一个程序传染、蔓延到不同的计算机。同时,使被传染的计算机程序、计算机、计算机网络成为计算机病毒的生存环境及新的传染源。

3. 潜伏性

计算机病毒具有依附于其他程序的寄生能力。依靠病毒的寄生能力,病毒传染给正常的程序和系统后,可能很长一段时间都不会发作,往往有一段潜伏期。病毒的这种特性是为了隐蔽自己,同时在隐蔽状态下去感染其他的程序,并伺机进行破坏行为。

潜伏性的另一个特征是其隐蔽性。隐蔽性是指计算机病毒一般都不独立存在,而是使用嵌入的方法寄生在一个正常的程序中。有一些病毒程序隐蔽在磁盘的引导扇区中,或者

磁盘上标记为坏簇的扇区中,以及一些空闲概率比较大的扇区中。这就是病毒的非法可存储性。处于潜伏期的病毒在满足了特定条件后就会显示其破坏特征。

4. 可触发性

处于潜伏期的计算机病毒在其环境满足一定的条件后才会被激活。病毒在具备了一个或多个条件后才会被激活,激活的实质是一种条件控制,病毒程序可以依据编写者的要求,在条件满足时实施攻击行为。具体的激活条件可以是输入特定字符,或者是某个特定日期或特定时刻,或者是病毒内置的计数器达到一定次数等。

5. 衍生性

根据编写者的事先设计,或者其他已经掌握该病毒编写代码的人员的有意修改,计算机病毒在发展、演变过程中可以衍生出一种或多种新病毒,这种新病毒被称为原病毒的变种。能够产生变种的病毒在传播过程中可以有效地隐蔽自己,使之不易被反病毒程序发现及清除。

4.1.4 计算机病毒的分类

计算机病毒不是一个独立存储并运行的文件,而是嵌入到一个宿主程序中并借助宿主程序的运行而运行的一段代码。根据病毒所依附的宿主程序的不同,可将计算机病毒主要分为可执行文件病毒、引导扇区病毒和宏病毒3种类型。

1. 可执行文件病毒

可执行文件(executable file)是指可以由操作系统进行加载执行的文件。在不同的操作系统环境下,可执行程序的呈现方式不同。例如,在Windows操作系统下,可执行程序可以是.exe文件、.sys文件、.com文件等类型。

可执行文件病毒嵌入在可执行文件中,当病毒感染了一个可执行文件时,病毒会修改原文件的一些参数,并将病毒自身程序添加到原文件中。当一个病毒嵌入可执行文件时,可嵌入在头部、尾部或插入在文件中间。

如果病毒嵌入在可执行文件的头部,当宿主程序被执行时,操作系统首先会运行病毒代码,然后再运行宿主程序。此类病毒较宿主程序优先取得了运行权,所以用户很难发现病毒的存在。如果病毒嵌入在可执行文件的尾部,病毒为了使自己具有优先运行权,必须修改宿主程序的参数,加入一条跳转指令,使得在宿主程序执行时首先跳转到病毒代码,执行完病毒代码后再运行宿主程序。当病毒插入在文件中间位置时,由于宿主程序被病毒一分为二,一方面需要采用零长度插入技术使得病毒的隐藏更加隐蔽;另一方面病毒插入后不能影响宿主程序的运行,同时还要使病毒优先于宿主程序运行,这对病毒的编写提出了更高的要求。

零长度插入技术是指病毒感染宿主文件时,将其病毒代码放入宿主程序,并不会增加宿主程序的长度,但能够实现攻击行为。此类病毒在感染时,采取了特殊方式,首先在宿主程序中寻找“空洞”(具有足够长度的全部为零的程序数据区或堆栈区),将病毒代码放入“空洞”中;然后改变宿主程序开始处的代码,使隐藏在“空洞”中的病毒代码能够优先运行,并在病毒运行结束时,恢复宿主程序开始处的代码;最后运行宿主程序。

方式,即当用户在浏览器中打开邮件时,其正文是一个 Web 页面。利用该工作机制,一些病毒便嵌入在 Web 代码中,当用户打开邮件时直接运行或待用户单击链接后自动下载。邮件附件是一些病毒主要的选择目标之一,当感染了病毒的邮件附件被用户下载后,病毒将进入用户所使用的计算机。利用共享文件夹传播感染了病毒的文件是一种常见的病毒传播方式,该方式不仅影响使用 NetBIOS 协议的 Windows“网上邻居”的文件共享,而且影响到使用 SMB 和 CIFS 共享及 P2P 共享,甚至是网盘共享等。利用文件共享机制,病毒还可以搜索可写的共享文件夹,并将自己复制到其中。

4.1.6 计算机病毒的防范方法

计算机病毒的防御需要通过建立有效的防范体系和管理制度,从技术、制度和习惯各个层面同时开展工作,具体可从预防、检测和清除 3 个方面进行计算机病毒的防御。

1. 病毒的预防

有效预防计算机病毒,可从以下几个方面加强管理或提高安全意识。

(1) 使用正版软件。正版软件一般有一定的安全保障,不会因为这些软件本身隐藏计算机病毒而感染计算机。

(2) 安装反病毒软件。在安装好操作系统后,首先要安装一套功能较为齐全的反病毒软件。

(3) 备份重要数据。为了防止重要数据被病毒修改后无法恢复,要养成对重要数据进行及时备份的习惯。

(4) 加强文件传输过程中的安全管理。不论是通过 U 盘等移动存储介质在计算机之间复制文件,还是通过网盘、邮箱等方式传输或转发文件,在打开文件之前一定要进行查病毒操作,防止这些文件里隐藏有病毒。

(5) 不打开可疑的 Web 链接。对于可疑的邮件附件、Web 链接,不要轻易打开。

2. 病毒的检测

由冯·诺依曼体系结构可知,计算机系统中所有信息最终均以二进制字节序列存储。因此,计算机病毒检测的实质就是一个依据相关规则与先验知识,通过某种算法对二进制(或十六进制)字节序列进行模式识别的问题。目前,常见计算机病毒的检测方法主要分为以下几种类型。

(1) 特征代码法。特征代码法是利用已经创建的计算机病毒的特征代码病毒样本库,在具体检测时比对被检测的文件中是否存在病毒样本库中存在的代码,如果有就认为该文件感染了病毒,并根据样本库来确定具体的病毒名称。

很显然,特征代码法的有效性建立在完善的病毒样本库的基础上。病毒样本库的建立需要采集已知病毒的样本,即提取病毒的特征代码。提取病毒特征代码的基本原则是:提取到的病毒特征代码具有独特性,即不能与正常程序的代码吻合;同时,提取到的病毒特征代码长度应尽可能小些,以减小比对时的空间和时间开销。

特征代码法的优点是检测准确、速度快、误报率低,且能够确定病毒的具体名称;但缺点是不能检测出病毒样本库中没有的新病毒。该方法在单机环境中的检测效果较好,但在网络环境中的检测效率较低。

4.2.1 网络蠕虫的特征与工作机制

计算机病毒、网络蠕虫(简称蠕虫)和木马都属于恶意代码,在蠕虫刚刚出现时将其作为计算机病毒对待,但在发展过程中蠕虫逐渐形成了其独有的特征和传播机制。

1. 网络蠕虫与计算机病毒之间的区别

自从 1988 年 Morris(莫里斯)蠕虫爆发后,为了区分蠕虫和病毒,对病毒重新进行了定义:计算机病毒是一段代码,能把自身加到其他程序包括操作系统上,它不能独立运行,需要由它的宿主程序运行来激活;而网络蠕虫是通过网络传播,无须用户干预且能够独立地或者依赖文件共享主动攻击的恶意代码,通过不停地获得网络中存在漏洞的计算机上的部分或全部控制权来进行传播。网络蠕虫强调自身的主动性和独立性,具有主动攻击、行踪隐蔽、利用漏洞、造成网络拥塞、降低系统性能、产生安全隐患、反复性和破坏性等特征。

2. 网络蠕虫的功能结构

网络蠕虫的功能结构包括主体功能和辅助功能两部分。其中,主体功能包括信息搜集模块、探测模块、攻击模块和自我推进模块 4 个模块;辅助功能包括实体隐藏模块、宿主破坏模块、通信模块、远程控制模块和自动更新模块 5 个模块。图 4-4 是网络蠕虫的功能结构,表 4-1 是对各功能模块的描述。

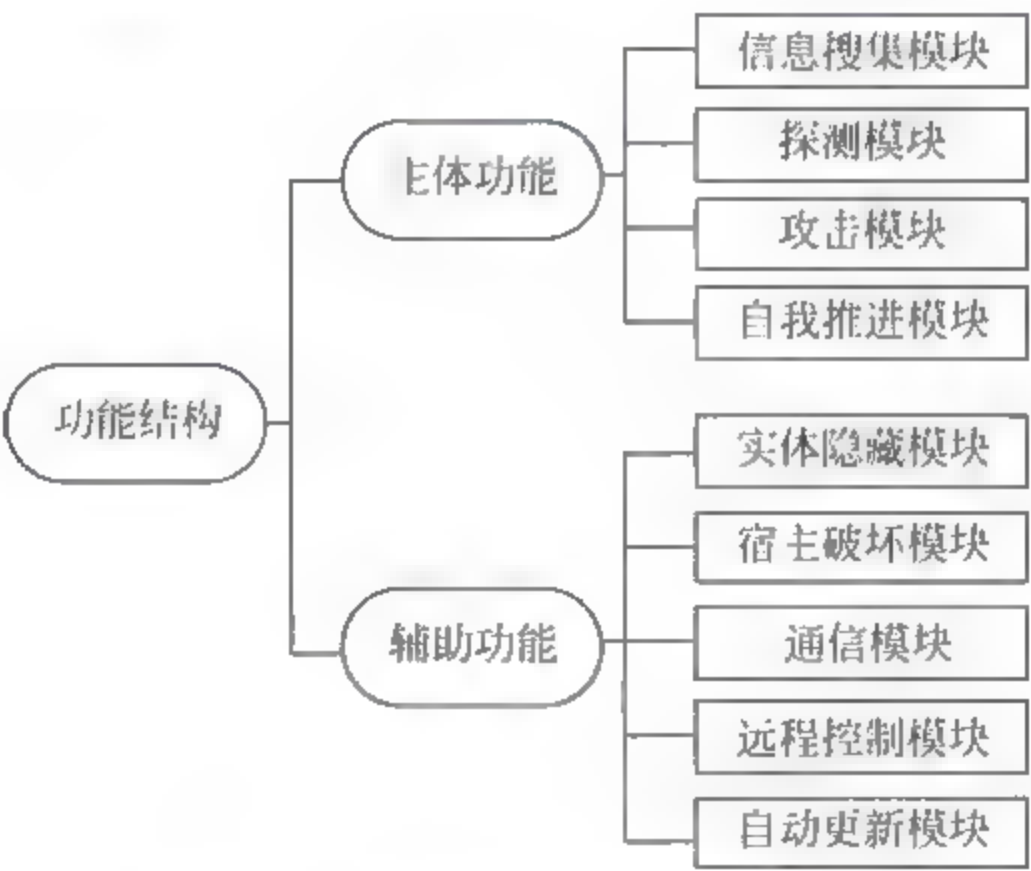


图 4-4 网络蠕虫的功能结构

表 4-1 网络蠕虫功能模块的描述

模块名称	功能模块的描述
信息搜集模块 (Information collection module)	决定对本地或目标网络进行信息搜集的算法,本机系统信息、用户信息、邮件列表、对本机信任或授权的主机、本机所处网络的拓扑结构、边界路由信息等
探测模块 (Probe module)	完成对特定主机的脆弱性检测,并决定采用哪种渗透方式发起攻击
攻击模块 (Attack module)	该模块利用获得的安全漏洞,建立传播途径。在攻击方法上是开放的、可扩充的

续表

模块名称	功能模块的描述
自我推进模块 (self propagating module)	该模块可以采用各种形式生成各种形态的蠕虫副本,在不同主机间完成蠕虫副本传递
实体隐藏模块 (Concealment module)	包括对蠕虫各个实体组成部分的隐藏、变形、加密及进程的隐藏,主要提高蠕虫的生存能力
宿主破坏模块 (Crash module)	该模块用于摧毁或破坏被感染主机,破坏网络正常运行,在被感染主机上留下后门等
通信模块 (Communication module)	该模块能使蠕虫间、蠕虫同黑客之间进行交流(这是未来蠕虫发展的重点);利用通信模块,蠕虫间可以共享某些信息,使蠕虫的编写者更好地控制蠕虫行为
远程控制模块 (Remote control module)	该模块的功能是调整蠕虫行为,控制被感染主机,执行蠕虫编写者下达的指令
自动更新模块 (Automatic updating module)	该模块可以使蠕虫编写者随时更新其他模块的功能,从而实现不同的攻击目的

3. 网络蠕虫的工作机制

网络蠕虫的工作机制如图 4-5 所示。通过前文对网络蠕虫功能结构的介绍,尤其是从网络蠕虫主体功能模块实现可以看出,网络蠕虫的攻击行为可以分为信息搜集(collect information)、探测(probe)、攻击(attack)和自我推进(self propagate)4 个阶段。其中,信息搜集主要完成对本地和目标节点主机的信息汇集,探测主要完成对具体目标主机服务漏洞的检测,攻击利用已发现的服务漏洞实施攻击,自我推进完成对目标节点的感染。

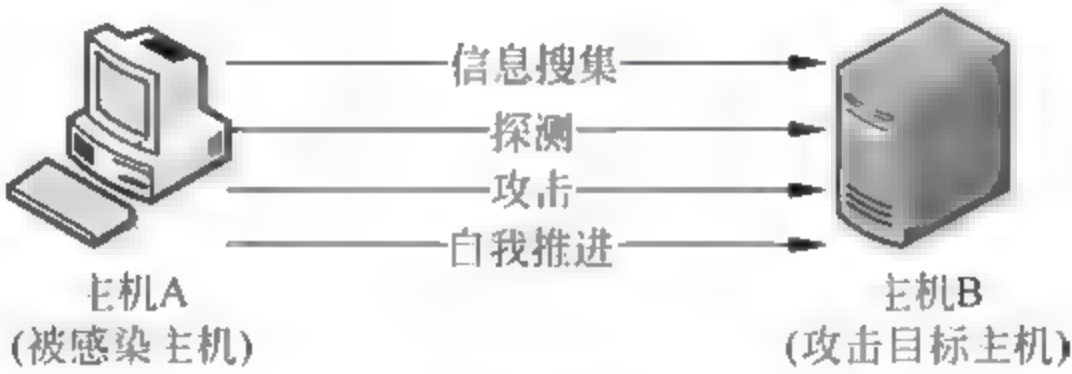


图 4-5 网络蠕虫的工作机制

4.2.2 网络蠕虫的扫描方式

蠕虫利用系统漏洞进行传播。在传播前首先要进行对攻击目标主机的探测,设计良好的扫描策略能够加速蠕虫传播。在 Internet 中,理想状态下一个通过精心设计的扫描策略能够使蠕虫在最短时间内找到全部可以感染的主机。按照对目标地址空间的选择方式的不同,可以将蠕虫的扫描方式分为以下几种类型。

1. 选择性随机扫描(selective random scan)

蠕虫在对目标主机进行扫描时,如果遍历所有的主机在 Internet 环境中几乎是不现实的,最可行的方式是有选择性地扫描。如果采取随机扫描方式,会对整个地址空间的 IP 随机抽取进行扫描,而选择性随机扫描将最有可能存在漏洞主机的地址集作为扫描的地址空间。选择性随机扫描也是随机扫描方式的一种。在选择性随机扫描中,所选的目标地

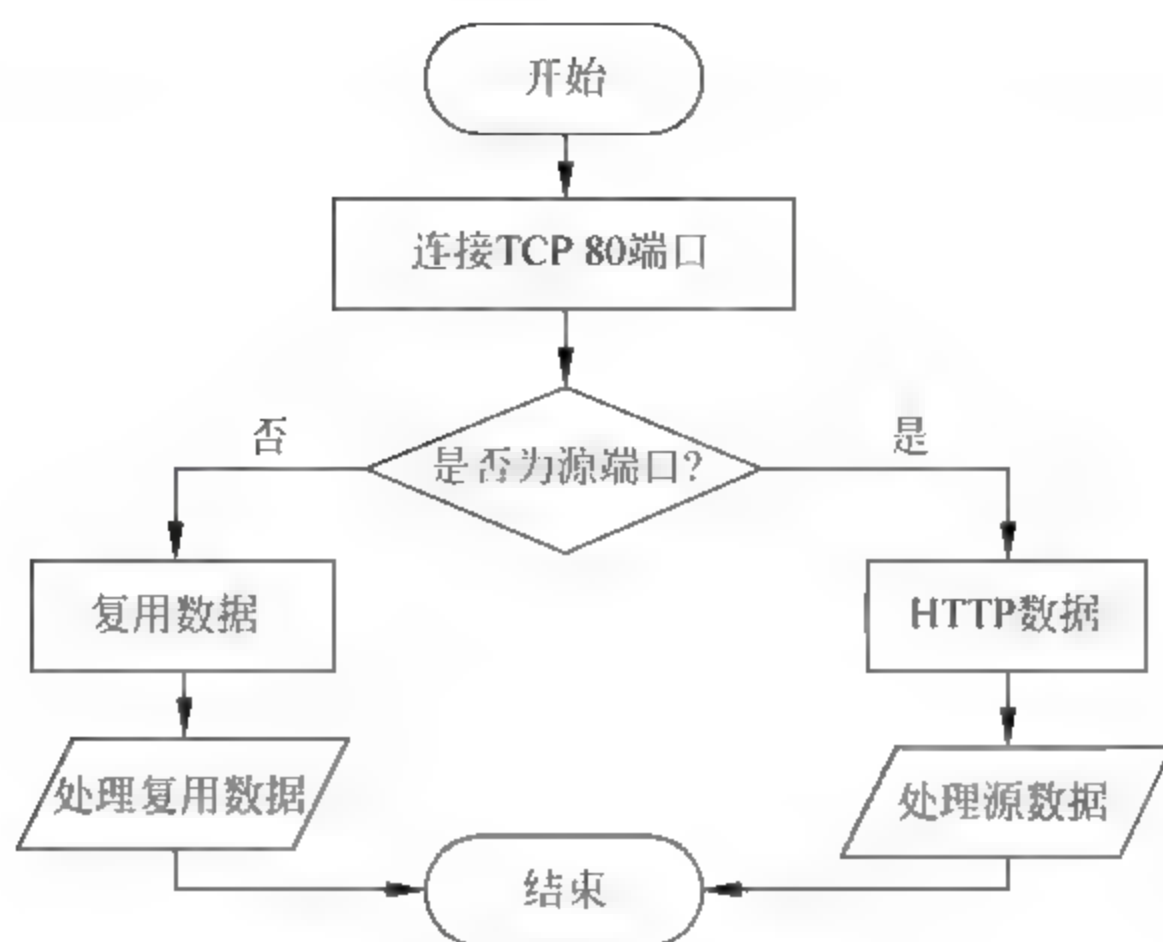


图 4-8 端口复用的实现过程

口、启动/停止服务等功能。例如,WinEggDropShell、Eternity 便是一个经典的扩展后门程序,它能实现进程管理(查看或结束进程)、注册表管理、服务管理(停止、启动等)、端口到程序关联、系统重启与注销、嗅探密码、重定向、HTTP 服务等功能。

4. C/S 后门

C/S(Client/Server)结构是木马主要使用的工作模式,同时也是后门程序的一种操作方式,尤其是具有控制功能的后门多采用该结构。ICMP Door 便是一种典型的 C/S 后门,它利用 ICMP 协议,通信过程中不需要打开任何端口,只是利用系统本身的 ICMP 包进行控制。ICMP Door 的另一个应用是实现从外网向内网的渗透,实现对网络内部主机的控制。由于 ICMP Door 使用了 ICMP 协议,如果主机启用了防火墙,则该后门程序将无法正常工作。

5. 账户后门

账户后门是指攻击者为了长期控制目标主机,通过后门在目标主机中建立一个备用管理员账户的技术。一般采用克隆账户方式来实现。克隆账户一般有两种方式:一种是手动克隆账户;另一种是使用克隆工具。

4.4.3 Windows 系统后门程序的自动加载方法

利用操作系统的自启动功能来加载后门程序是攻击者最常使用的方法。在 Windows 系统中,后门工具可以利用自启动文件夹、注册表自启动项和 Windows 服务等方式来达到自启动目的。

1. 自启动文件夹

能够实现程序自启动的文件夹有两种类型:当前用户专用启动文件夹和所有用户共用启动文件夹。当前用户专用启动文件夹位于“\Users\[用户名]\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup”下,其中“用户名”是当前登录的用户账户名;所有用户共用启动文件夹位于“Documents and Settings\All Users\开始菜单\程

内的所有成员都可以看到。

综上所述,可以将僵尸网络定义为:攻击者(bomaster)出于恶意目的,通过传播僵尸程序(bot)来控制大量主机(肉鸡),并通过一对多的命令与控制(C&C)信道所组成的网络。

一对多的命令与控制信道是僵尸网络区别于其他攻击方式的最基本的特征。图 4-9 是一个僵尸网络的结构。其中,被安装在受控主机上的僵尸程序能够把自己复制到一个安装目录,并通过改变系统配置实现开机运行功能。攻击者应用事先设定的登录方式登录到 C&C 服务器(如 IRC 服务器)中的指定频道,向所有连接到该频道的僵尸程序发布命令。

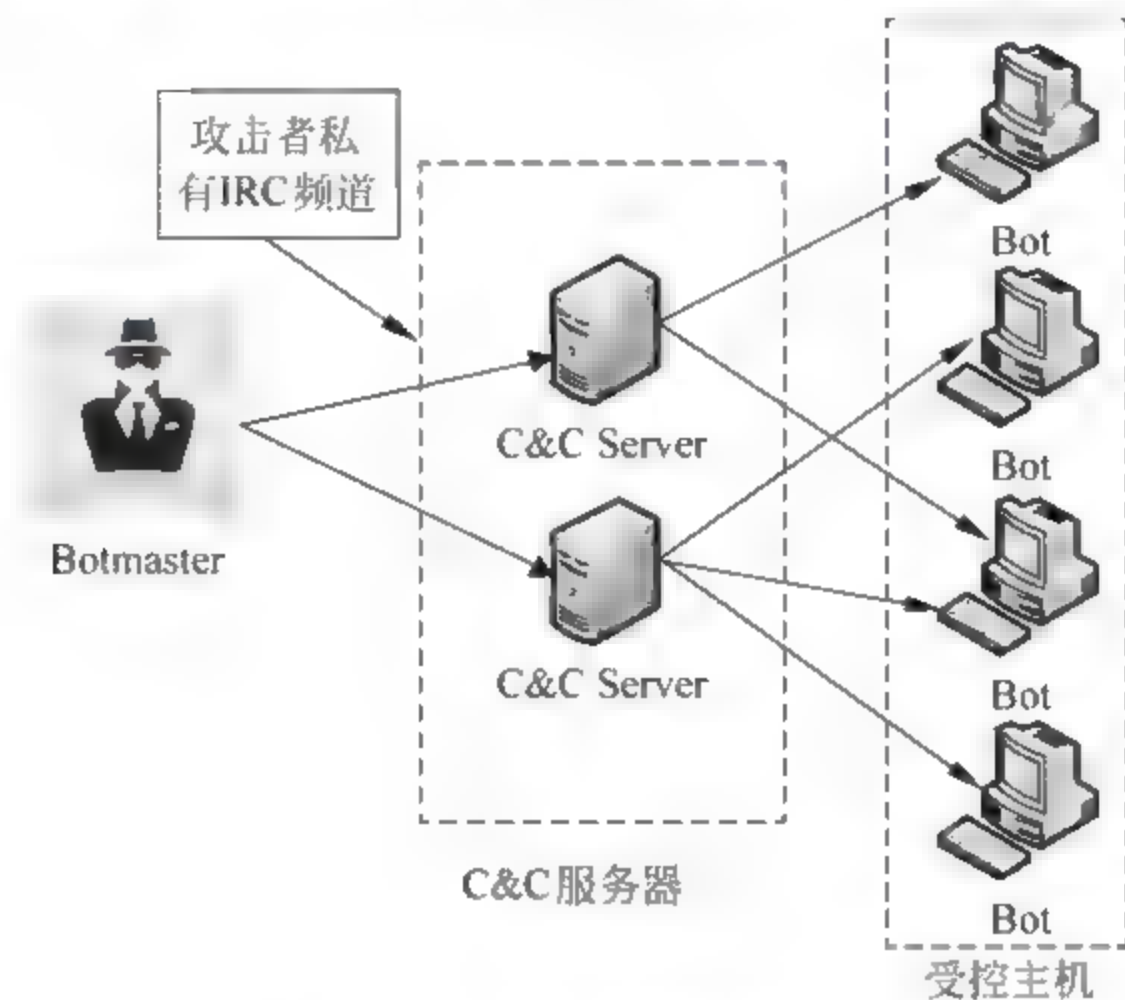


图 4-9 僵尸网络的结构

需要特别说明的是,在上述介绍中,僵尸网络的命令与控制机制是基于 IRC 协议实现的,这是因为僵尸程序的起源可追溯到 1993 年出现的“Eggdrop Bot”。Eggdrop 的功能类似于智能机器人(robot,简写为 bot),用于帮助 IRC 网络管理员更加高效地管理网络,没有以攻击网络为目的。但从 1998 年出现的 GTBot 开始,它利用 IRC 协议构建命令与控制频道,其程序中内嵌了一个流行的 IRC 客户端 mIRC.exe 可用于僵尸程序。自此,基于 IRC 协议的僵尸网络开始流行,如 Sdbot、PrettyPark、Spybot、Rbot、Agobot 等。但是在基于 IRC 协议的僵尸网络的发展过程中,大量局域网开始在位于边界的防火墙上通过过滤与 IRC 协议相关的端口以防御僵尸网络的攻击,致使僵尸网络逐渐使用 HTTP、P2P、Domain Flux、Random P2P、Fast flux、Hybrid P2P 等协议作为命令与控制协议,以应对被检测和封堵的风险。鉴于对僵尸网络基本工作机制的理解,本节主要以 IRC 协议为主进行介绍。如果读者需要更加全面地学习有关僵尸网络的知识,可在学习本节内容后再参阅相关的文献。

4.5.2 僵尸网络的功能结构

最早出现的 IRC 僵尸网络由僵尸网络控制器(Botnet Controller)和僵尸程序(Bot)两部分组成。由于 IRC 僵尸网络基于标准 IRC 协议构建其命令与控制信道,所以其控制器可构建在公用 IRC 聊天服务器上,但攻击者为保证对僵尸网络控制器的绝对控制权,一般会利用其完全控制的主机架设专门的僵尸网络命令与控制服务器。

在僵尸网络中,根据攻击过程中所发挥功能的不同,可以将僵尸程序的功能模块分为主

体功能模块和辅助功能模块两部分,其组成如图 4-10 所示。

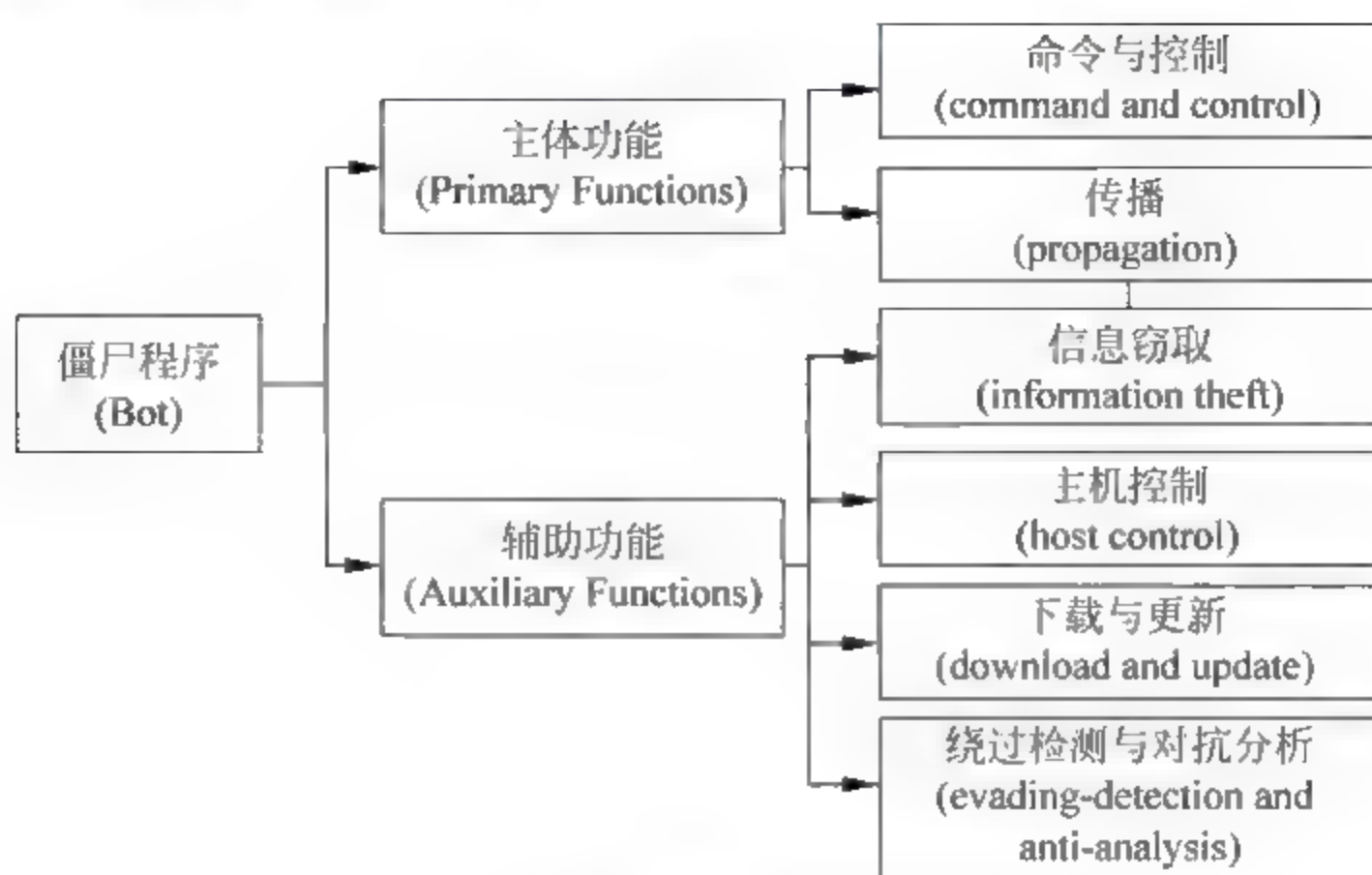


图 4-10 僵尸网络的功能结构

1. 僵尸程序的主体功能

主体功能是僵尸程序的主要组成部分,僵尸网络的主体功能分为命令与控制 and 传播两个模块。

(1) 命令与控制。命令与控制(C&C)模块是整个僵尸程序的核心,用于实现与僵尸网络控制器的交互,接收攻击者的控制命令,进行解析和执行,并将执行结果反馈给僵尸网络控制器。

(2) 传播。传播模块通过各种不同的方式将僵尸程序传播到新的主机,使其加入僵尸网络接受攻击者的控制,从而扩展僵尸网络的规模。僵尸程序可以按照传播策略分为自动传播型僵尸程序和受控传播型僵尸程序两大类,而僵尸程序的传播方式包括通过远程攻击软件漏洞传播、扫描 NetBIOS 弱密码传播、扫描恶意代码留下的后门进行传播、通过发送邮件病毒传播、通过文件系统共享传播等。此外,最新的僵尸程序也已经开始结合即时通信软件和 P2P 文件共享软件进行传播了。

2. 僵尸程序的辅助功能

僵尸程序的辅助功能是对主体功能的补充,主要包括信息窃取、主机控制、下载与更新、绕过检测与对抗分析等功能模块。

(1) 信息窃取。信息窃取模块用于获取受控主机信息,主要包括系统资源情况、进程列表、开启时间、网络带宽和速度等。同时,搜索并窃取受控主机上有价值的敏感信息,如软件注册码、电子邮件列表、账号口令等。

(2) 主机控制。僵尸网络中的主机控制模块是攻击者利用受控的大量僵尸主机(肉鸡)完成各种不同攻击目标的模块集合。目前,主流僵尸程序中实现的僵尸主机控制模块包括 DDoS 攻击模块、架设服务模块、发送垃圾邮件模块及单击欺诈模块等。

(3) 下载与更新。下载与更新模块为攻击者提供向受控主机注入二次感染代码及更新僵尸程序的功能,使其能够随时在僵尸网络控制的大量主机上更新和添加僵尸程序及其他恶意代码,以实现不同攻击目的。

(4) 绕过检测与对抗分析。绕过检测与对抗分析模块包括对僵尸程序的多态、变形、加密、通过 Rootkit 方式进行实体隐藏,以及检查调试程序(debugger)的存在、识别虚拟机环境、杀死反病毒进程、阻止反病毒软件升级等功能。其目标是使得僵尸程序能够绕过受控主机的使用者和反病毒软件的检测,并对抗反病毒软件的检测,从而提高僵尸网络的生存能力。

HTTP 僵尸网络与 IRC 僵尸网络的功能结构相似,所不同的仅仅是 HTTP 僵尸网络控制器是以 Web 网站方式构建。而相应地,僵尸程序中的命令与控制模块通过 HTTP 协议向控制器注册并获取控制命令。由于 P2P 网络本身具有的对等节点特性,在 P2P 僵尸网络中也不存在只充当服务器角色的僵尸网络控制器,而是由 P2P 僵尸程序同时承担客户端和服务器的双重角色。P2P 僵尸程序与传统僵尸程序的差异在于命令与控制模块的实现机制不同。

4.5.3 僵尸网络的工作机制及特点

攻击者在选择受控主机时,一般会利用漏洞扫描技术来发现互联网中存在安全漏洞的主机,并获得管理员的权限。当成功攻陷主机后,攻击者把编写好的僵尸程序利用 FTP、HTTP、TFTP 或 DCC SEND(IRC 用来给其他用户发送文件的命令)上传到主机,并通过配置系统进行自动安装。当僵尸程序成功安装后,它就会连接预先设定的频道,等待攻击者发送命令。在许多情况下,攻击者为了防止某一个频道被发现后使已建立的僵尸网络被破坏,通常会利用动态域名映射方式,把 IRC 服务器映射到动态 IP,让僵尸程序加入动态的频道或多个频道。攻击者登录到频道,发布命令实施各种攻击活动。

1. 僵尸网络的工作机制

基于 IRC 协议的僵尸网络的工作机制如图 4-11 所示,具体过程如下。

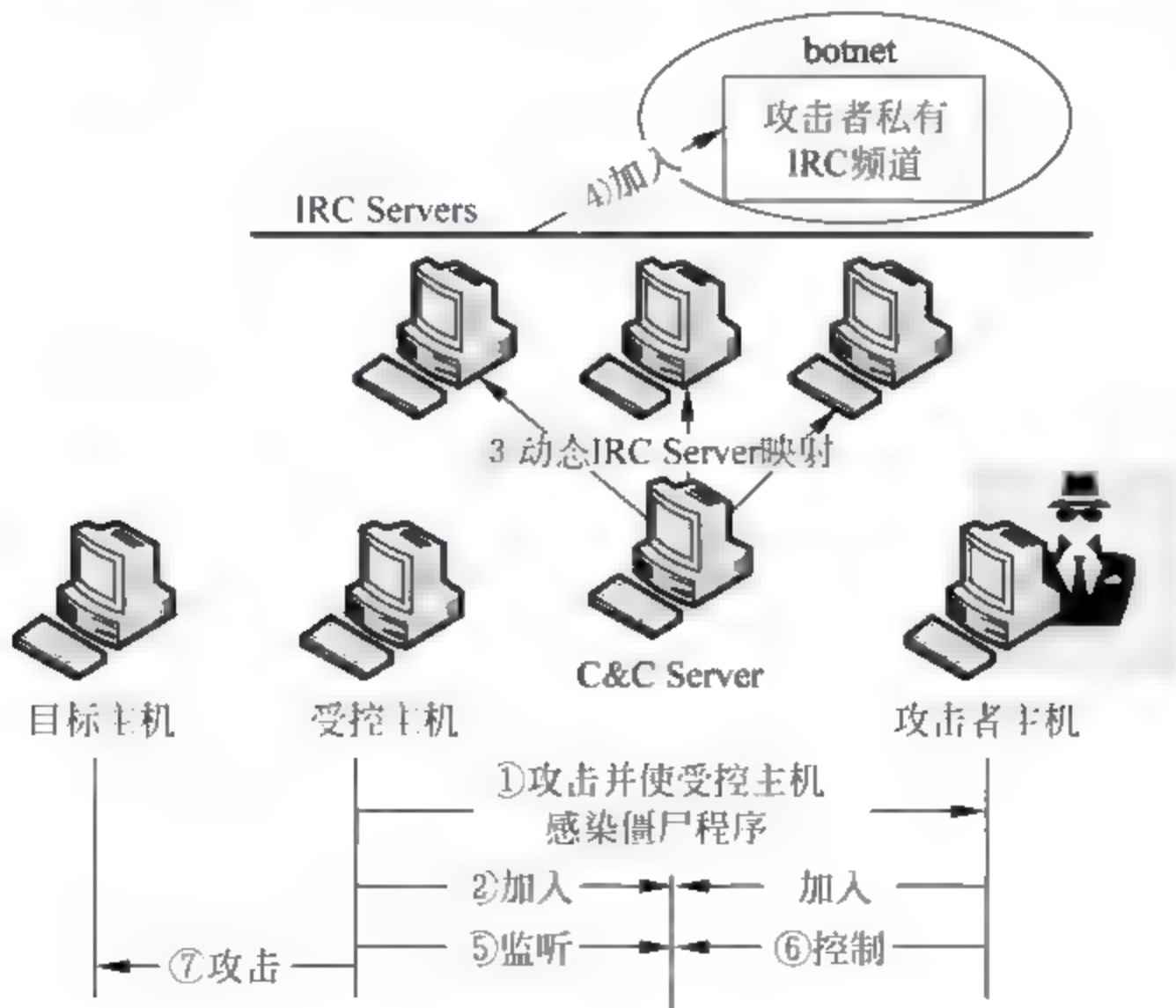


图 4-11 IRC 协议的僵尸网络的工作机制

1. 僵尸网络的跟踪

充分了解僵尸网络的内部工作机制是防御者应对僵尸网络安全威胁的前提条件。僵尸网络跟踪(botnet tracking)为防御者提供了一套可行的方法,其基本思想是:首先通过各种途径获取因特网上实际存在的僵尸网络命令与控制信道的相关信息;然后模拟成受控的僵尸程序加入僵尸网络中,对僵尸网络的内部活动进行观察和跟踪。

部署包含有蜜罐主机的蜜网(honeynet)是对僵尸网络进行跟踪的一种有效方法。利用蜜网,可以捕获到因特网上实际传播的大量僵尸程序,然后分析出僵尸程序所连接的 IRC 命令与控制信道信息,包括 IRC 服务器的域名及 IP 地址和端口号、连接 IRC 服务器的密码、僵尸程序用户标识和昵称的结构、加入的频道名和可选的频道密码等。然后,使用 IRC 客户端追踪工具根据控制信道信息加入到僵尸网络进行跟踪。

通过对僵尸网络的跟踪,可以较为全面地了解僵尸网络的控制服务器位置、行为特性和结构特性,为防御者进一步检测与处置僵尸网络提供了充分的信息支持。不过也存在一些不足:基于蜜罐技术的采集和跟踪方法无法有效地检测出全部活跃的僵尸网络,无法为因特网用户提供直接保护;另外,僵尸网络控制者在觉察到被跟踪后,可以采取信息裁减机制、更强的认证机制等方法加大僵尸网络跟踪的难度,并减少跟踪所能够获取的信息;还有,各种基于 HTTP 协议和基于 P2P 协议的僵尸网络命令与控制机制的使用为僵尸网络跟踪带来了较大困难;最后,防御者对僵尸网络实施跟踪一旦被发现,就很可能被僵尸网络控制者实施 DDoS 攻击。

2. 僵尸网络的防御与反制方法

僵尸网络的防御与反制是一项较为复杂的工作,下面介绍常用的几种方法。

(1) 传统防御方法。由于构建僵尸网络的僵尸程序仍是恶意代码的一种,所以传统的防御方法是加强因特网主机的安全防御等级以防止被僵尸程序感染,并通过及时更新反病毒软件特征库清除主机中的僵尸程序,主要包括使用防火墙、DNS 阻断、补丁管理等技术手段。

(2) 创建黑名单。通过路由和 DNS 黑名单的方式屏蔽僵尸网络中恶意的 IP 地址和域名是一项简单而有效的技术。在该方法中,如何获得恶意 IP 地址及域名等信息是关键。目前,已有一些研究机构和个人在网络上共享了通过僵尸程序分析、IDS 日志分析等方法获得的恶意 IP 地址和域名的黑名单。为此,只要能够确保黑名单的及时性和准确性,创建黑名单方法是非常有效的。

另外,针对基于 Web 方式来传播僵尸程序这一现象,目前各主流的 Web 浏览器都加入了黑名单机制来阻止用户对恶意 Web 网址的访问。例如,Google 公司启动了 Google Safe Browsing 项目来收集并发布挂马和僵尸程序宿主网页及钓鱼网站,并以黑名单的形式集成在 firefox 和 chrome 浏览器中。其他浏览器厂商也进行了类似的工作。

(3) 关闭僵尸网络使用的域名。直接关停僵尸网络所使用的域名或关闭其命令与控制服务器的网络连接是一种最直接有效的方法。例如,针对僵尸网络具有命令与控制信道这一基本特性,可以通过摧毁或无效化僵尸网络命令与控制机制使其无法对因特网造成危害。

4.6 Rootkit

Rootkit 不是一项新技术,但却是恶意代码家族中发展最快、安全威胁最大的技术之一。McAfee 实验室在“McAfee Labs Threats Predictions for 2017 And Beyond”中提出:硬件和固件将日益成为通过复杂技术进行攻击的主要目标。Rootkit 技术涉及 UNIX/Linux、Windows、NetWare 计算机操作系统,以及 Google Android、Apple iOS、Windows Phone 等移动智能终端操作系统。

4.6.1 Rootkit 的概念

从网络攻击的方法来看,Rootkit 是攻击者使用的一个软件工具集,用于获得对系统的非授权访问,为攻击者获取敏感数据提供特殊权限,并隐藏自己的存在,而且根据需要允许安装其他恶意软件。从 Rootkit 的组成 Root(特权用户)和 kit(工具集)可以看出,Rootkit 是能够获得系统特权并能够控制整个系统的工具集。在安装 Rootkit 之前,攻击者需要管理员权限。Rootkit 是最具挑战性的恶意软件,因为它很难通过系统提供的检测机制及第三方的检测软件发现。

综上所述,Rootkit 是一种能够同时针对操作系统(包括微内核操作系统)的用户模式和内核模式进行程序或指令修改,达到通过隐藏程序执行或系统对象的变化来规避系统正常检测机制、绕开安全软件监控与躲避取证手段,进而实现远程渗透、尝试隐藏、长期潜伏并对整个系统进行控制的攻击技术。与传统的恶意代码不同,Rootkit 攻击的灵活性更大、破坏性更强、被检测的难度也大,当然技术要求更高。

Rootkit 与计算机病毒、蠕虫、木马、后门和僵尸程序等同属于恶意代码,都是由攻击者按照攻击意图植入到被攻击系统中的程序或代码,都具有潜伏性和破坏性。但与其他类型的恶意代码不同的是:Rootkit 还会替换或修改被攻击系统中的程序。作为恶意代码家族中的新秀,Rootkit 几乎集成了家族成员所有的优势:破坏性最强的计算机病毒会修改硬件 ROM 中的代码(如 CIH 病毒),而这是 Rootkit 最基本的特征。木马最大的特点是将自己伪装成为合法的程序,以便能够用欺骗方式隐藏自己,而 Rootkit 的隐藏性要比传统的木马更深;木马程序通过远程 Shell、远程控制 GUI 等方式对被攻击系统实施远程控制,并为攻击者绕过正常的安全检测机制提供访问通道,更能在系统重启后实施自启动,在这方面 Rootkit 是有过之而无不及的。作为一种特殊形态的恶意代码,Rootkit 能够将自己伪装为系统中的一个合法程序(木马的特征),使得攻击者可以按照自己的方式去访问系统(后门的特征),修改或替换硬件(如 BIOS、显卡等)中的代码或系统中的正常程序而将自己隐藏起来(高级计算机病毒的特征)。

4.6.2 用户模式 Rootkit 和内核模式 Rootkit

自底向上分层模型的特点是通过层间接口技术将下层的差异性利用统一的服务模式(标准或协议)封装起来,下层为其上层提供一种抽象一致的按需服务。然而,这种分层模型却为攻击者提供了可利用的机会,攻击者通过篡改下层组件结构或劫持并替换下层组件的

运行。更为可怕的是,攻击者可以通过对两次中断劫持中攻击方式的组合,实施更复杂、破坏性更强的攻击。例如,在第1次中断劫持后获得对系统底层的控制权,而在第2次劫持后可以获取对操作系统的控制权,实施对内核的 Rootkit 攻击。

4.6.4 挂钩技术

虽然 Rootkit 可以攻击操作系统的用户模式,但其核心功能还是以攻击内核模式为主。同时,为增加技术分析时的针对性,本节主要以 Windows Rootkit 为分析对象。

Windows 系统采用基于事件驱动的消息传递机制。Windows 系统将事件封闭在消息中,信息是系统用于告诉应用程序某个事件发生的一个通知,如用户移动鼠标、按下键盘等都作为一个事件而产生一个信息,系统将信息传递给指定的窗口进行处理,这样基于事件驱动的信息传递机制便实现了 Windows 应用程序 GUI 界面的交互。在以上的过程中,系统内部具体执行了哪些操作,内部的程序又是按什么顺序运行的,用户并不知道。

挂钩(Hooking)技术是将要执行的具有某种特殊功能的代码(如 Rootkit 攻击代码)作为外挂程序巧妙地插入到目标程序(被挂钩程序)中。当目标程序执行到被挂钩处时强行转向执行外挂程序(钩子程序),当外挂程序执行结束后再返回目标程序的被挂钩处继续执行目标程序。挂钩技术能够为用户提供系统或进程中各种事件产生的消息,并能够根据用户需要改变程序的执行流程,且增加新的功能。也就是说,挂钩技术为用户访问 Windows 系统程序的结构和执行方式提供了一种途径,而 Windows 系统的这一工作机制却为实现 Rootkit 攻击创造了条件。攻击者只要能够访问目标进程的地址空间,就可以挂钩并修改其中的任何函数(如函数指针、系统调用入口地址等)。在进程打开时这些被修改后的函数被调用执行,此时将自动跳转到攻击者设置的攻击代码所在的地址去执行,并实现隐藏进程和端口等功能。例如,利用挂钩技术,攻击者可以将木马、后门等恶意代码以驱动程序的形式挂钩到系统的正常启动流程中(如 Windows 的 Winload.exe),使这些恶意代码在用户根本不知情的情况下随着系统驱动程序的加载而自动运行。

从理论上讲,不管是用户模式还是内核模式,只要存在能够挂钩的地方都可以实现基于挂钩的 Rootkit 攻击。

1. API 函数挂钩攻击

API 函数挂钩是最典型的一种挂钩技术。在 Windows 环境下主要有两种实现 API 函数挂钩的操作:一种是通过修改 PE(Portable Executable,可移植执行体)文件的 IAT(Import Address Table,输入地址表)使 API 函数地址重定向,该方式称为 IAT Hooking(基于 IAT 表的挂钩);另一种是篡改 API 函数地址中的机器码,即用无条件跳转指令 JMP 的机器码来替换 API 函数入口地址中的机器码,该方式称为 Inline Hooking。

(1) IAT Hooking。输入函数是指允许被程序调用,但其自身却不在调用程序中的函数。Windows 系统中的输入函数执行体一般位于一个或多个动态链接库(DLL)中,当 PE 文件被调入内存时,Windows 加载程序才会加载 DLL,即通过 DLL 来调用输入函数。IAT 表中就保存着调用函数与输入函数地址之间的关联信息。如图 4-13 所示,Rootkit 攻击程序会分析内存中目标程序(PE 文件)的结构,用 GetProcAddress 获取 API 函数的地址,根据该地址在 IAT 表中查找目标函数(输入函数)的地址,然后用 VirtualProtect 改变内存区域的保护,之后再用攻击函数地址替换 IAT 表中该条目中目标函数地址。最后,当目标函

数被调用时,实际执行的是攻击函数,而非原函数。该攻击方式实现起来较为容易,但对使用 GetProcAddress 显式调用的 DLL 不起作用。

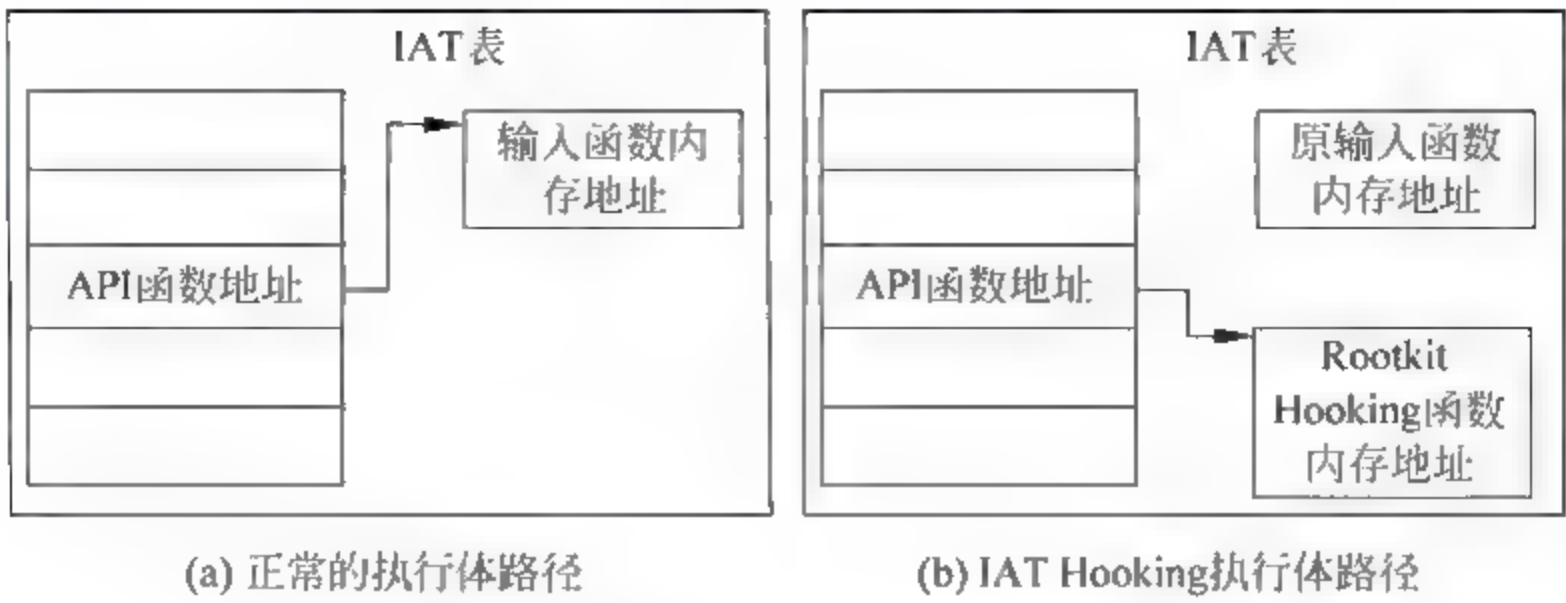


图 4-13 IAT Hooking 的工作过程

(2) Inline Hooking。与 IAT Hooking 通过修改内存中输入函数地址实现到 Rootkit 攻击函数跳转不同的是: Inline Hooking 直接修改 API 函数入口处的机器码使其转到 Rootkit 攻击函数。在进行了跳转后,为了使 API 函数能够顺利执行,在完成 Rootkit 攻击函数执行后还须返回 API 函数,接着执行 API 函数后续的代码。Inline Hooking 的工作过程如图 4-14 所示。该攻击方式的通用性强,从理论上可以在 API 函数的任何地方把原来指令替换成 Rootkit 攻击者的跳转指令,来躲避在线(inline)检测。但缺点是由于不同操作系统中的机器码可能不同,所以攻击函数的稳定性和跨平台操作效果较差。

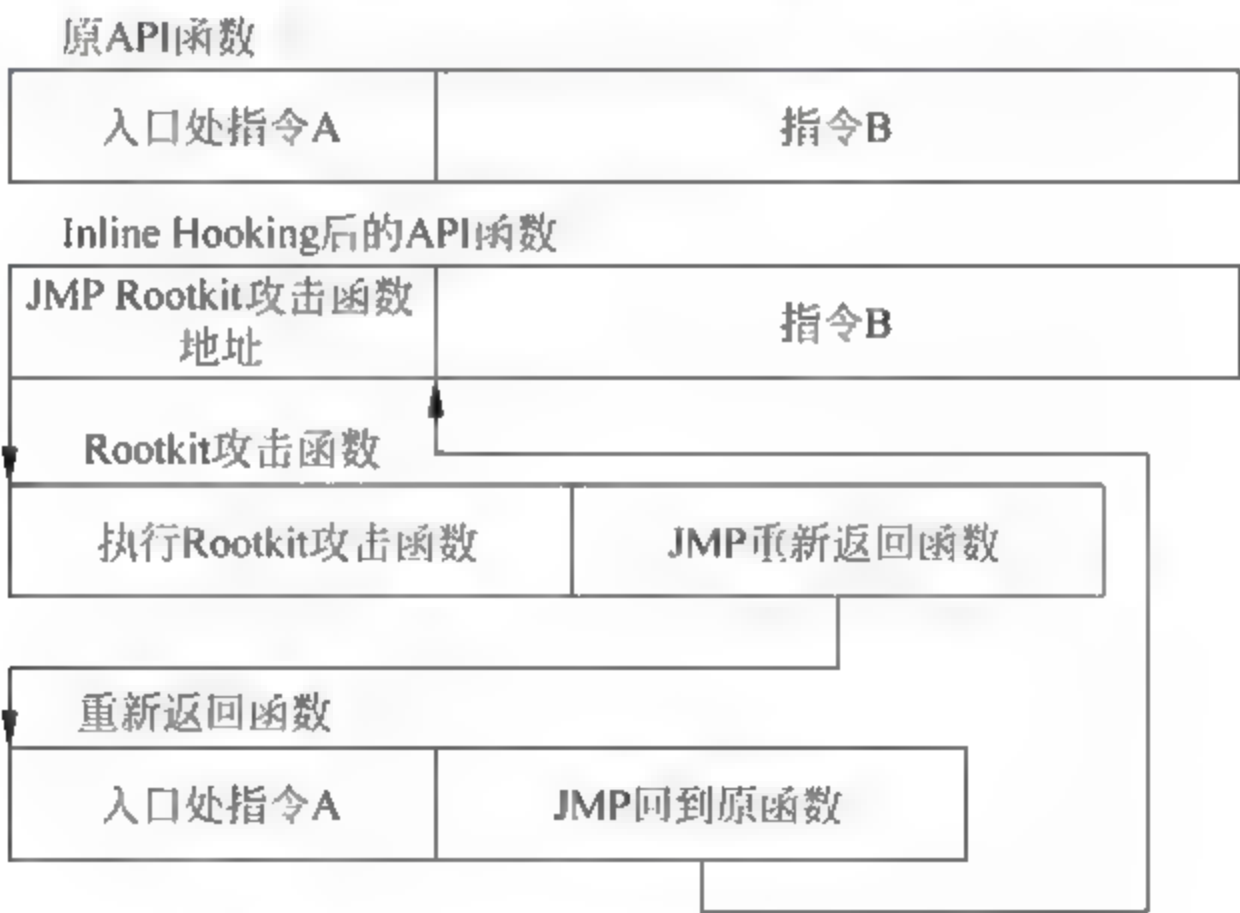


图 4-14 Inline Hooking 的工作过程

2. 描述符表挂钩攻击

Rootkit 攻击者可以针对 SSDT、IDT、GDT、LDT 等描述符表(Descriptor Table,DT)的挂钩机制,对操作系统内核进行攻击。

(1) SSDT 挂钩攻击。SSDT(System Service Descriptor Table,系统服务描述符表)是 Windows 系统中实现用户程序调用系统服务的查询表,即关联用户模式下的 Win32 API 与内核模式下的系统服务函数的关联表。可以将被应用程序调用的系统服务函数的服务号及对应的入口地址存放在 SSDT 表中,这样当应用程序向操作系统发送了一个调用系统服务

在 Windows 系统默认状态下,GDT 和 LDT 都包含有调用门(call-gates)入口,GDT/LDT Hooking 的实现方式是在描述符表保留字段中插入一个调用门描述符来改变内在段的执行特权,再借助相关技术实现进程隐藏。由于每个实际运行的处理器分别对应一个 GDT 表,每个线程可以获得其对应进程所包含的 LDT 表的相应内容,在 GDT/LDT Hooking 攻击中,攻击者首先会设计一个包含 Rootkit 攻击代码的调用门,然后将该调用门插入到 GDTR 寄存器的 GDT 指定位置。同时,当一个任务发生切换时,包含 Rootkit 攻击代码的线程管理器用攻击程序线程的 LDT 表替换正在运行线程的 LDT 表,实现对线程的隐藏。

(4) IRP 挂钩攻击。IRP(I/O Request Package,I/O 请求包)是 Windows 内核中一个预定义的数据结构,一个 IRP 由一个固定的首部和不定数目的 IRP 栈单元块组成,IRP 栈为先进后出的向下生长的栈。当上层应用程序需要调用底层的 I/O 设备时,应用程序便发送一个 I/O 请求,I/O 管理器首先将其转换为一个 IRP,然后传送到合适的驱动程序栈中的不同派遣例程进行处理。IRP 用 IoGetCurrentIrpStackLocation 函数获取指向当前栈单元的指针,使用 IoCopyCurrentIrpStackLocationToNext 或 IoSkipCurrentIrpStackLocation 函数把当前栈单元复制到下一个栈单元。

基于 Windows 系统的层次模型和 IRP 栈先进后出的工作机制,驱动程序使用 IoSetCompletionRoutine 函数挂接一个完成例程,而该完成例程信息存储在对应驱动程序的 IRP 栈单元中。攻击者将 Rootkit 驱动程序插入到驱动程序栈中,在截获合法驱动程序后对其信息进行修改和过滤,从而达到隐藏文件、嗅探击键和鼠标操作等目的。

4.6.5 DKOM 技术

前面介绍的 API 函数挂钩攻击和描述符表挂钩攻击都是利用被攻击对象的工作机制,通过修改程序执行流程或重定向指令等方式来实现 Rootkit 攻击。而 DKOM(Direct Kernel Object Manipulation,直接内核对象操作)Rootkit 攻击技术通过直接修改 Windows 系统的设备驱动程序或可加载内核模块,以实现进程、文件和网络连接的隐藏和进程提权。

以 Rootkit 攻击者实现 Windows 系统进程隐藏为例。当创建一个进程时,系统会给该进程建立一个对应的内核 EPROCESS 结构,该结构的第一个成员为 KPROCESS;当创建一个线程时,系统同样会建立一个对应的内核 ETHREAD 结构,该结构的第一个成员为 KTHREAD。在 EPROCESS 结构体中,有一个类型为 LIST_ENTRY 结构体的成员 ActiveProcessLinks,它是一个拥有 FLINK 和 BLINK 两个指针成员的双链表节点,两个指针成员分别指向前后两个进程 EPROCESS 结构体的 ActiveProcessLinks 成员。当需要隐藏 Rootkit 攻击代码的进程时,只需要把该进程的 EPROCESS 结构体从双向链表中移除即可,如图 4-16 所示。

4.6.6 虚拟化技术

早期的 Rootkit 一般通过 Hooking 技术改变程序的执行路径、过滤系统调用的返回信息,或者直接采用 DKOM 技术篡改系统内核对象来实现攻击过程,对操作系统的运行具有较大的依赖性,所以无法彻底消除 Rootkit 攻击过程产生的痕迹,容易被基于操作系统的检测技术发现。硬件虚拟化技术的出现导致了与操作系统无关的恶意软件的出现,如基于虚

习 题

1. 什么是恶意代码？主要包括哪些类型？
2. 什么是计算机病毒？具有什么基本特征？并简述其感染和传播机制。
3. 简述可执行文件病毒、引导扇区病毒和宏病毒的特点和工作机制。
4. 什么是蠕虫？它与计算机病毒之间的区别是什么？
5. 简述网络蠕虫的传播机制。
6. 什么是木马？它与计算机病毒和蠕虫之间的区别是什么？
7. 简述网页木马的攻击过程及特点。
8. 什么是后门？它与计算机病毒和木马之间的区别是什么？
9. 分析端口复用技术在网络攻击中的实现方法。
10. 在熟悉 Windows 自启动实现方法的基础上，通过实际操作，测试其实现过程。
11. 与计算机病毒、蠕虫、木马、后门等恶意代码相比，僵尸网络在实施攻击的方式上有什么特点？
12. 简述僵尸网络的工作机制，并分析其防御方法。
13. 什么是 Rootkit 技术？与传统的恶意代码相比，具有哪些特点？
14. 简述 Rootkit 攻击的实施方案。
15. 什么是挂钩技术？
16. 什么是 API 函数挂钩攻击？分析 IAT Hooking 和 Inline Hooking 之间的区别。
17. 什么是描述符表挂钩攻击？介绍 SSDT、IDT、GDT、LDT 的实现方法。
18. 什么是 DKOM 技术？介绍其实现方法。
19. 通过对 Rootkit 攻击技术的介绍，简述其检测和防御方法。
20. 挖矿木马有什么特征？如何进行有效防范？

(1) 基于并发请求数量拒绝 IP 地址。如果同一个客户端的并发连接数量超过此处的设置值,就拒绝其连接。

(2) 基于一段时间内的请求数量拒绝 IP 地址。如果同一个客户端,在指定时间内的连接数量超过此处的设置值,就拒绝其连接。

习 题

1. 简述 C/S 结构和 B/S 结构的特点。
2. Web 应用安全涉及哪些具体内容,简述其安全防范方法。
3. 为什么在对 Web 服务器实施攻击之前需要进行信息的收集? 具体应收集哪些内容? 如何收集?
4. 简述网络踩点、网络扫描和网络查点的功能,并通过具体操作掌握其应用。
5. 简述 PING 命令的功能,并介绍如何使用 PING 来探测一台主机的连通性。
6. 在熟悉 TCP 和 UDP 协议工作原理的基础上,分别简述基于 TCP 和 UDP 协议进行主机扫描的方法。
7. 在熟悉端口概念和应用分类的基础上,简述端口扫描的功能及常见的 TCP 和 UDP 端口扫描的实现方法。
8. 什么是系统类型探测? 分别简述操作系统类型和网络服务类型探测的实现原理,并借助工具软件(如 nmap 等)进行实验测试。
9. 漏洞扫描的工作原理是什么? 漏洞扫描器是如何工作的? 简述漏洞扫描器各组成部分的功能。
10. 什么是网络查点? 它与网络踩点、网络扫描之间存在什么关系,介绍常见的网络查点方法。
11. 针对 Web 服务器的各类信息收集攻击,如何进行有效防范?
12. 互联网环境中的敏感数据主要包括哪些内容? 如何加强对敏感数据的管理?
13. 什么是网站篡改? 如何进行防范?
14. 什么是内容注入和 SQL 注入? 简述 SQL 注入攻击的实现原理和具体过程,并介绍其防范方法。
15. 什么是跨站脚本漏洞与跨站脚本攻击? XSS 攻击分为哪几类? 如何有效防范 XSS 攻击?
16. 针对 Web 服务器软件的攻防,分别介绍 Apache 和 IIS 服务器的安全配置方法。

第6章 Web浏览器的攻防

随着博客(blog)、微博(microblog)、社交网站(Social Networking Site, SNS)、Web 2.0等一系列新型应用的产生,基于B/S(Browser/Server,浏览器/服务器)架构的Web应用越来越广泛。同时,随着移动互联网应用的不断普及,Web功能也在随着应用环境的变化而不断发展和完善,以满足用户的新需求。与此同时,伴随着Web应用需求的迅速发展,也引起了攻击者的强烈关注,攻击者利用Web前端(Web浏览器)和Web后端(Web网站操作系统、Web应用程序和Web服务器软件)的安全漏洞实施攻击,已经对正常的Web应用安全构成了严重威胁。本章主要关注Web浏览器的安全,在介绍Web浏览器相关知识的基础上,重点介绍Web浏览器的攻防技术。

6.1 Web浏览器技术

目前,用户间的交流、文件上传与下载、网上交易、信息检索与浏览等操作都集中在Web浏览器(Web Browser)上实现,Web浏览器成为互联网中应用最为广泛的客户端软件。

6.1.1 万维网

1989年12月,蒂姆·伯纳斯·李(Tim Berners Lee)发明了万维网(World Wide Web, WWW),指出:HTTP(Hyper Text Transfer Protocol,超文本传输协议)和HTML(Hyper Text Markup Language,超文本标记语言)就是计算机之间交换信息时所使用的语言,也就是说当用户在计算机上单击一条链接时,用户的计算机就会自动进入想要查看的页面,之后它就会利用这种计算机之间的语言与其他计算机进行沟通。随后,他又将WWW的发明称为:这是新时代的敲门声,这是新生命的呼吸和心跳,这是全人类的你、我、他。

WWW并非某种特殊类型的计算机网络,而是在互联网(Internet)上通过HTTP和HTML等协议,实现的一个大规模的、联机式的分布式信息应用。所以,WWW是基于互联网的一类应用。WWW的应用具有以下明显的特点。

(1) 超链接。通过超链接(Hyper Link)实现了一个网页与另外一个网页的关联,能够方便地从一个网页访问另一个网页(即网页之间的链接),这些网页文件可以在同一个站点,也可在不同的站点。

(2) 超文本和超媒体。通过超链接将多个文本组合起来形成超文本(Hyper Text)。早期的超文本已经发展为后来的超媒体(Hyper Media),因为早期的WWW应用大都包含着文本信息,而后来在此基础上增加了图形、图像、声音、动画、视频图像等内容,即通过超链接将多媒体或流媒体文件链接起来,组合成了超媒体。

(3) 客户服务器方式。WWW以客户服务器方式工作,其中浏览器就是在用户计算机

上的 WWW 客户端程序,保存 WWW 文档并运行服务软件的计算机称为服务器。客户端程序向服务器端程序发出请求,服务器端程序向客户端程序返回所需要的 WWW 文档。在一个客户端程序提供的窗口中显示出的 WWW 文档称为网页(page)。

(4) 统一资源定位符(URL)。为了标志分布在互联网上的 WWW 文档,使用了 URL (Uniform Resource Locator,统一资源定位符)。通过 URL,能够使每一个文档在整个互联网的应用范围内具有唯一的标识。URL 的一般语法格式如下:

```
<协议>://<主机>[:端口]/<路径>/[;参数][?查询]
```

其中,带方括号[]的为可选项。

(5) 超文本传输协议(HTTP)。为了实现 WWW 上文档之间的链接,使客户端程序能够与服务器端程序之间进行交互,提出了超文本传输协议(HTTP)。HTTP 是一个应用层协议,它使用 TCP 连接进行可靠的数据传输。

HTTP 协议传输的数据都是未加密的明文数据,存在安全隐患。为了保证用户隐私数据在传输过程中不被泄露,网景公司设计了 SSL(Secure Sockets Layer,安全套接层)协议用于对 HTTP 协议传输的数据进行加密,从而出现了 HTTPS。简单地讲,HTTPS 协议是由“SSL+HTTP”协议构建的可进行加密传输、身份认证的具有安全加密特征的网络协议。

(6) 超文本标记语言(HTML)。超文本标记语言(HTML)实现了不同功能和风格的 WWW 文档在互联网不同计算机上的显示,并且可以使网页设计者方便地以“链接”方式从一个页面的指定位置关联到互联网上任何一个页面。HTML 不是应用层的协议,而是一种制作 WWW 网页的标准语言,它消除了不同计算机之间信息资源存在的障碍。发布于 2014 年 9 月的 HTML 5.0 增加了在网页中嵌入音频、视频以及交互式文档等功能,目前一些主流的浏览器都支持 HTML 5.0。

下面是与 HTML 有关的两种语言。

① XML(eXtensible Markup Language,可扩展标记语言)。XML 和 HTML 都是标准通用标记语言的子集,其中 HTML 被设计用来显示数据,而 XML 被设计用来传输和存储数据。具体地讲,XML 用于标记电子文件,可以对文档和数据进行结构化处理,是一种允许用户对自己的标记语言进行定义的源语言。XML 不是替代 HTML,而是对 HTML 应用功能的补充。

② XHTML(Extensible Hyper Text Markup Language,可扩展超文本标记语言)。XHTML 是一个基于 XML 的标记语言,它综合了部分 XML 的强大功能及大多数 HTML 的简单特性,是一个扮演着类似 HTML 角色的 XML。更具体地来讲,XHTML 的功能与 HTML 类似,只是语法结构更加严格,是作为一种 XML 被重新定义的 HTML,并将逐渐取代 HTML。目前新的浏览器都支持 XHTML。

6.1.2 Web 浏览器

1990 年蒂姆·伯纳斯-李推出了第一款被称为“World Wide Web”的命令行的 Web 浏览器软件。1991 年 5 月,WWW 结合了 Web 浏览器后在诞生于 19 世纪 60 年代的 Internet 上首次露面,立即引起轰动,获得了极大的成功,被广泛应用。

1. 国外 Web 浏览器的发展

1993 年 2 月被称为“Mosaic”的全球第一个图形界面浏览器(Browser)推出。“Mosaic”项目的负责人 Marc Andreessen 在大学毕业后创办了网景公司,并在 Mosaic 的基础上研发了 Netscape 浏览器。

在网景公司的 Netscape 浏览器取得成功的同时,微软公司意识到了 Web 浏览器在互联网快速发展中所起的巨大作用,所以从 Spyglass 公司取得了 Mosaic 源代码授权,在 1995 年推出了 Internet Explorer(IE)浏览器,并通过 Windows 操作系统捆绑推广,并迅速抢占了 Netscape 的市场份额,成为市场占有率最高的 Web 浏览器。

网景公司与微软公司在 Web 浏览器竞争中失利后,开放了 Netscape 浏览器的源代码,成立了非正式组织 Mozilla,并推出了 Firefox 浏览器(也称为“Mozilla Firefox 浏览器”),继续与 IE 浏览器进行竞争。

2008 年 9 月,Google 公司推出了 Chrome 浏览器,以快速、简单、安全的特点很快赢得用户的青睐。基于开源内核的 Chrome、Firefox、Safari(Mac OS 中的浏览器)等浏览器丰富了 PC 端用户上网的应用需求。与此同时,微软公司意识到了开源内核浏览器带来的竞争压力,在频繁更新 IE 版本(2011 年发布 IE 9,2012 年发布 IE 10,2013 年发布 IE 11)之后,重新开发了名为“Edge”的浏览器来取代 IE。

2. 国产 Web 浏览器的发展

1999 年一个网名为“changyou”(畅游)的程序员在论坛上发布了一款名为“MyIE”的浏览器,标志着国产 Web 浏览器的诞生。MyIE 基于 IE 开发,并进行了性能优化和功能扩展。在 MyIE 源代码的基础上,开发了 TheWorld(世界之窗)浏览器,该浏览器后来被 360 公司收购后发展为现在的 360 安全浏览器。目前,国产浏览器主要有 360 安全浏览器、猎豹安全浏览器、傲游浏览器、百度浏览器、腾讯 TT 浏览器等。

自从 Web 浏览器出现后,国内用户长期以来主要使用 IE,尤其是网上银行、各类在线支付系统以及大多数网站的页面显示都是在 IE 的基础上开发的,部分使用新内核的浏览器则无法正常浏览。在此情况下,一方面为了继续使用原来在 IE 下开发的系统,同时能够使用到新内核浏览器带来的功能,便出现了“双核浏览器”。所谓双核,是指一个浏览器同时拥有两个内核,用户可以根据应用需要进行切换。由于 IE 在国内用户中特殊的地位,“双核”中的一个内核一般是 Trident(IE 使用的内核),其他内核可采用 Webkit(Safari、Chrome 使用该内核)、Chromium(Google 创建的基于 Webkit 内核的开源浏览器引擎)、Gecko(Firefox 使用该内核)、Presto(Opera 7.0 及以上版本使用该内核)等。其中,使用“Trident”内核时称为“兼容浏览模式”,而使用其他内核时称为“高速浏览模式”。

需要说明的是:国内双核浏览器是迫于网络应用环境而产生的一个过渡产物,随着 Web 标准的普及,双核浏览器自然会失去存在的意义。

6.1.3 Web 浏览器的安全

Web 浏览器应用的广泛性和产品的多样性在丰富了用户上网体验的同时,也增加了安全风险。与其他应用软件相比较,由于网上银行、在线支付等应用都通过 Web 方式进行,Web 浏览器存在的安全风险已对用户财产和个人隐私构成严重威胁。

由于B/S结构同时涉及Web客户端(主要包括客户端操作系统和Web浏览器)、Web服务器端(主要包括服务器端操作系统、Web服务器软件和Web应用软件)和应用层协议(主要包括HTTP/HTTPS和FTP),系统运行过程中涉及的环节较多,环境相对复杂,所以涉及的安全问题较多,而且部分安全威胁可能同时涉及B/S的多个方面。例如,针对Web浏览器的攻击与渗透,具体实施时可能同时涉及客户端操作系统和运行在该操作系统上的Web浏览器。

仅Web浏览器自身来说,由于不同的浏览器采用的内核存在着差异,而且每一款浏览器都几乎通过功能扩展来体现各自的特色,因此Web浏览器缺乏一个可供大家遵循的严格的安全规范,这成为Web浏览器安全隐患产生的根源。同时,HTML、XHTML、CSS等语言和规范存在的安全漏洞,以及JavaScript、Flash、PHP、SilverLight等客户端运行环境存在的安全风险,都会使Web浏览器的安全变得非常复杂。

大多数Web浏览器用户都希望浏览器能够通过扩展程序、插件和浏览器帮助对象(Browser Helper Objects,BHO)提供一些便利。但是,这些附加产品在通过将组件添加到浏览器的默认功能来提高用户感受的同时,也成为恶意攻击者的首要攻击目标。因为用户在修补和更新插件和扩展程序方面的能力普遍较差,而且第三方扩展插件的开发过程一般缺乏安全保障,同时浏览器插件一般也不具备版本自动更新的机制,安全漏洞被利用的时间周期要比系统软件以及浏览器软件本身长。虽然很多主流的附加组件是由知名供应商所开发的,但是任何人都可以写一段代码让这些组件成为传递恶意软件的潜在工具。因此,浏览器就成为了终端最脆弱的攻击目标。另外,软件漏洞的利用一般需要在软件运行状态下进行,而浏览器长期处于联机运行状态,为攻击提供了便利。

Web浏览器旨在为用户提供一些扩展程序的权限控制,但是通常会因为粗粒度访问控制而被攻击。另外,用户总是对各种附加产品授予权限,防风险意识不强。很多用户认为一个附加产品托管在官方扩展程序库中就想当然认为它是安全的,不过尽管大多数附加产品在推出之前都要经过审查,但是违反浏览器开发者意图的恶意扩展程序并不少见。例如,提交给苹果扩展程序库的苹果Safari扩展程序其实托管在一个外部位置,而Mozilla Firefox允许来自第三方网站扩展程序的安装等。

Web浏览器的安全风险主要涉及浏览器URL地址栏欺骗攻击、浏览器URL状态栏欺骗攻击、浏览器页面标签欺骗攻击、浏览器页面解析欺骗攻击、浏览器插件安全、浏览器本地存储安全、浏览器安全策略被绕过、浏览器隐私安全、浏览器差异带来的安全风险等方面。

6.1.4 Web浏览器的隐私保护

隐私保护是网络攻防领域一个备受大家关注的问题。虽然在网络攻击过程中不会直接利用到用户的隐私,但隐私是攻击前信息收集的主要内容。为此,有效保护隐私对加强网络防范是非常有必要的。本节重点介绍Web浏览器应用中的隐私泄露与保护问题。

目前,许多Web浏览器自身存在着严重的隐私泄露问题。浏览器会收集用户的上网行为(如什么时候访问过什么网站),并且把用户的上网行为信息保存在自己的服务器上,然后再通过大数据分析,了解每一位上网用户的个人爱好、上网习惯等信息。因为用户上网信息中蕴藏着大量的商业利益,所以一些公司和商业机构出于自身利益会大量收集用户的上网

信息。其中,一些浏览器厂商的绝大部分收益依靠“在线广告”。要实现广告的在线精准投放,自然要收集用户的信息,只有浏览器厂商在对用户的上网信息收集并分析后,才知道哪些上网用户对哪些内容(广告)感兴趣。这期间就涉及了隐私问题。

与隐私有关的另一个问题是 Web 浏览器会记录用户的上网行为。例如,某一用户平时喜欢访问某一网站或在网搜索了某一内容(如某本书,某款式的服装等),但在操作了浏览器后没有消除浏览器的历史缓存,当下一次打开该 Web 浏览器时,就会发现之前查看的信息显示在页面中。

DNT(Do Not Track,请勿跟踪)是浏览器提供的一项禁止对用户上网行为进行跟踪的功能。DNT 功能可以在 HTTP 头部进行设置,当用户通过浏览器选择了这个功能(图 6-1),就可以免于被第三方网站跟踪网络痕迹。在 IE 11 中,也可以在“安全”选项卡下,选取“启用‘Do Not Track’请求”和“启用跟踪保护”来实现此功能。目前,IE、Firefox、Safari、Chrome、Opera 浏览器都支持该功能,但一般需要用户在选取后才会生效。

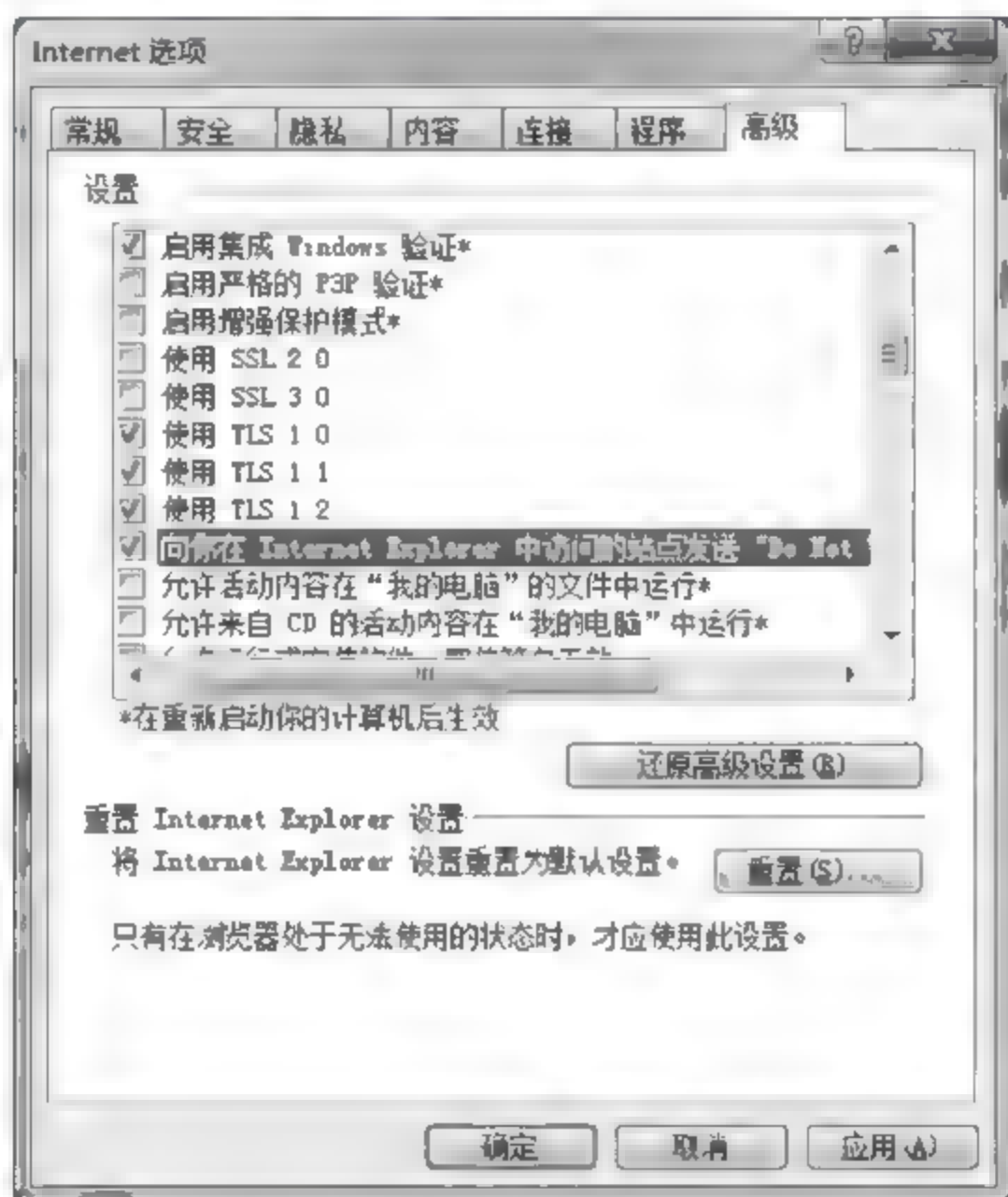


图 6-1 IE 11 中对“Do Not Track”功能的设置

保护用户隐私的另一种方法是使用浏览器的“隐私浏览模式”。当浏览器处于“隐私浏览模式”时,浏览器将不会保存相应的历史记录,在用户关闭了浏览器后所有浏览信息将自动消失。例如,当用户临时需要使用别人的计算机上网,但不想让别人知道自己访问过哪些网站时,就可以使用“隐私浏览模式”。目前,大部分浏览器都支持“隐私浏览模式”,在 IE 11 下,可以通过选取“安全”选项卡中的“InPrivate”来启用“隐私浏览模式”,将打开如图 6-2 所示的浏览窗口。

不过,如果用户的浏览器安装了插件,可能会导致“隐私浏览模式”下某些插件照样会留下上网痕迹。



图 6-2 浏览器处于“隐私保护模式”

6.1.5 Web 开放数据挖掘形成的安全威胁

互联网自身所具有的开放特质使得大量不同结构类型的数据暴露在互联网上,可以利用爬虫等工具采集、存储、追踪特定行为或人员的细节数据,即可实现开放数据挖掘。这种方法一旦被不法分子应用到对网站的攻击中,将构成巨大的安全威胁。

攻击者盗取网站后台数据库后,便可利用其中的注册信息、用户个人信息、隐私信息等牟取非法利益,甚至实施犯罪。近年来,不法分子利用互联网的开放特点,将目光转向挖掘网站上的公开数据,从而实施对所掌握数据的验证、确认等,某种程度上为辅助实施网络欺诈等侵害行为提供便利。

过去,不法分子搜集获取网民信息需要拖库或撞库等操作,其过程较为复杂。尤其是目前越来越多的网站对安全程度的重视明显提升,使得拖库和撞库越来越困难。而利用互联网上开放的数据,攻击者利用爬虫可以抓取用户的留言数据,“别有用心”的不法分子可以了解很多需要的信息。此外,微博上的个人信息、QQ 及 QQ 空间、微信及微信“个人相册”上的某些信息也是可以开放访问的,这些都为社会工程学手段提供了唾手可得的数据来源。

随着“互联网+”行动战略的实施,一方面,传统互联网公司业务快速扩展,另一方面将线下的商业机会与互联网结合的 O2O(Online to Offline,在线离线/线上到线下)新兴公司一批批上市,网民用户下载并注册的 APP,加上常用的大型购物、社交网站,已经达到几十甚至百余个。用户大量的隐私、非隐私但有识别身份价值的数据,都已暴露在公共互联网的开放环境中。

以手机号码为例,微信、淘宝、支付宝、QQ、微博、网易邮箱、360 手机卫士等都全部支持使用手机登录、修改密码。如果测试一个手机号码是否在目标网站注册过,只要在登录系统使用一下该号码即可。有些攻击者还可以利用网站查询端口批量测试一组号码是否在目标网站上注册,甚至可综合其他信息推测用户的大致偏好。

开放数据保护与利用是镜子的两面,就像隐私保护和让渡隐私增强个性化体验一样,需

要网站所属企业、安全厂商,以及监管三方共同努力。而从技术角度来讲,网站的防护思路也需要转变,例如,及时检测和避免公开数据被恶意抓取,采取技术手段强化数据安全存储与传输等。这些都将成为研究者和安全厂商未来的研究方向。

6.2 Web 浏览器插件和脚本的攻防

Web 浏览器被称为是访问互联网的入口,是当前使用最为广泛的客户端软件。伴随着 Web 浏览器的发展,其功能也在不断扩展。然而,Web 浏览器有些功能的扩展是通过业界共同遵循的标准来实现的,这类功能扩展方式具有普遍性,而有些功能的扩展因 Web 浏览器的不同而不同,具有差异性。

6.2.1 Web 浏览器插件的攻防

插件(Plug in 或 add in)又称为外挂,是针对某一特定系统平台、按照一定的规范编写的程序。插件一般不能单独运行,只能运行在程序规定的特定系统平台(某些插件可能同时支持多个平台)下,这是因为插件在运行时需要调用宿主程序提供的函数库或者数据。

1. 插件的特点

浏览器插件能够丰富浏览器的上网功能,是对浏览器应用功能的一种补充,如 Flash 插件能够让浏览器更好地展现网页中的动画内容,视频类插件为浏览器带来观看网络视频的功能,网银插件能够帮助用户在浏览器上方便完成支付等。然而,种类繁多的浏览器插件是一把双刃剑,在给用户带来上网便利和浏览网页效果的同时,也会带来严重的安全问题,其中基于浏览器插件的安全漏洞便是最严重的安全隐患。

为什么会存在插件呢?主要目的是扩展 Web 浏览器的功能,但该功能只是针对某一或某些特定系统或平台,而不具备普遍性。应用软件(如 Web 浏览器)为插件的加载和运行提供了应用程序接口和相关的服务功能,通过插件加载功能可以将插件安装到应用程序中,并实现应用程序与插件之间的数据交换。插件必须依赖于应用程序(宿主程序)才能发挥自身功能,单独依靠插件是无法正常运行的。反之,应用程序并不需要依赖插件就可以运行。

使用插件技术,可有利于应用程序的设计、开发和功能扩展,主要表现在以下几个方面。

(1) 结构清晰,易于理解。由于不同插件之间是相互独立的,因此结构非常清晰,也更容易理解。

(2) 可维护性强。由于插件与宿主程序之间通过接口联系,根据需要进行删除、插入或修改,结构较为灵活,软件的升级和维护较为方便。

(3) 可移植性好。因为插件本身就是由一系列功能模块组成的,并通过接口向外部提供自己的服务,所以插件可移植性好。同时,插件可以直接调用操作系统的 API,以动态链接库(Windows 操作系统上为 dll 文件)方式加载到浏览器的进程中。

(4) 便于功能扩展。实现应用程序功能的扩展,只需相应地增删插件,而不影响整个体系结构。

(5) 插件之间的耦合度较低。插件之间以及插件与宿主程序之间的信息交换都是通过插件与宿主程序间的通信来实现的,所以插件之间的耦合度更低。

(6) 插件的开发方式较为灵活。可以根据资源的实际情况来调整开发方式,资源充足时可以开发所有的插件,资源相对匮乏时可以选择开发部分插件,也可以请第三方的厂商开发,用户也可以根据自己的需要进行开发。

Web 浏览器能够直接调用插件程序,用于处理特定类型的文件。常见的 Web 浏览器插件有 Flash 插件、RealPlayer 插件、MMS 插件、MIDI 五线谱插件、ActiveX 插件等。根据插件在 Web 浏览器中的加载位置,可以分为工具条(Toolbar)、浏览器辅助(BHO)、搜索挂接(URL Searchhook)和下载 ActiveX 等方式。以 IE 为例,常见的插件程序的扩展名主要有 .ocx、.dll、.cab 和 .exe 几种类型,其中以 .exe 为扩展名的插件在安装前需要得到用户的授权,只有授权同意后才能下载安装,而其他 3 种扩展名的插件一般在浏览网页时在后台自动安装,用户可能无法察觉。

由于插件是用操作系统的本地代码编写的,并调用操作系统的 API,因此插件的行为浏览器是无法控制的。以 Flash 插件的 Cookie 为例,网页中的 Flash 文件可以利用 Cookie 在操作系统中保存一些信息,这时,即使浏览器使用了“隐私浏览模式”,因为浏览器无法限制插件的 Cookie,插件的 Cookie 同样会记录用户的部分上网信息,带来隐私问题。

2. 恶意扩展程序

浏览器是用户使用计算机上网的主要工具。为了增强浏览器的灵活性和易用性,很多浏览器都开放了一些标准扩展接口,供第三方开发者开发各种实用的扩展程序和浏览器插件。以 360 浏览器为例,可支持视频、邮件、截图、游戏、社交、阅读、抢票、购物、网银等多种类型的个性化功能扩展(图 6-3),开发者可以通过 360 安全浏览器应用开放平台提交自己开发的扩展应用,通过审核后即可在 360 浏览器的扩展中心中发布。



图 6-3 360 浏览器提供的个性化功能扩展

与正常的扩展程序不同,恶意扩展程序通常具有某些特定的攻击功能,一旦被植入浏览器,就会恶意篡改浏览器设置,劫持浏览器主页或劫持新建标签页,甚至篡改浏览器的扩展功能,而用户又无法卸载这些恶意扩展。恶意扩展程序的这些恶意行为对用户正常上网构成了严重的骚扰和安全威胁。

早期的恶意扩展程序主要是针对 IE 内核的浏览器,它们又被称为恶意插件。而随着 Chrome 内核浏览器及国内流行的双核浏览器应用的普及,针对 Chrome 内核的恶意扩展程序开始出现。从现有的恶意扩展案例看,这些恶意扩展主要以篡改浏览器主页为主要目的。

从恶意扩展程序的恶意行为可以看出,商业利益是催生恶意扩展程序的主要原因。某些正规合法企业也在从事恶意扩展程序的研发和推广,或者是借助恶意扩展程序来强制用户使用自己的产品。

3. 恶意插件的防范方法

有些插件程序能够帮助用户更方便地浏览网上信息或调用上网辅助功能,但也有部分程序被人称为恶意插件,常见的有广告软件(adware)和间谍软件(spyware)。此类恶意插件程序监视和收集用户的上网行为,并将收集到的信息自动发送给插件程序的开发者或攻击者,以达到投放广告、盗取银行账号密码等非法目的。以插件的安全防范为主,下面介绍几种有关 Web 安全的防范技术和方法。

1) 沙箱

为了防止攻击者通过浏览器对用户本地硬盘和注册表等进行访问,可以采用沙箱技术进行有效防范,从而消除对系统的危害。沙箱(sandbox)是一个基于虚拟机技术的系统程序,允许用户在沙箱环境中运行浏览器或其他程序,程序运行过程和结果都被隔离在指定的沙箱环境中,运行所产生的变化可以随后删除。沙箱通过虚拟出一个独立作业环境,使其内部运行的程序不会对沙箱外的环境(如硬盘)产生永久性的影响。运行在沙箱中的程序不能运行任何本地的可执行程序,不能从本地计算机文件系统中读取任何信息,也不能向本地计算机文件系统中写入任何信息。

沙箱技术最早用来测试不受信任的应用程序,目前还广泛应用于 Web 页面的安全浏览。当沙箱技术应用到安全访问 Web 网页时,无论何时加载远程网站上的代码并在本地执行,都不会威胁到用户本地的安全。

2) 自动更新

如果没有特殊的应用要求,浏览器应该始终开启自动更新功能。不过,并不是所有插件都会自动更新。例如,许多浏览器会自动更新 Adobe Flash 插件,但是大部分其他扩展程序需要通过运行相关产品的安装程序进行更新。

出于安全考虑,可以禁止运行已经过时的插件。目前,有些浏览器插件检测工具(如 Qualys 公司的 BrowserCheck)可以检查用户浏览器安装的插件,确定哪些插件需要更新,并针对过期插件提供更新下载链接。

3) 利用黑白名单

为了有效降低 Web 浏览器扩展程序的安全风险,可以将所有的插件先添加到指定的黑名单,然后选择性地添加一些必要的插件到白名单。为了尽可能降低安全风险,可以通过安全评估,将经常遭到攻击的安全性较差的插件从计算机中完全卸载,如果某些业务应用程序必须使用该插件,可以创建一个虚拟机,让这些不安全的插件在相对隔离的虚拟机环境中运

行。例如,针对安全漏洞较多的 Adobe Reader,可以使用集成在浏览器的 PDF 阅读器(如 Firefox 浏览器的 Mozilla PDF 阅读器)来替代 Adobe 版本。

另外,因为插件程序由不同的发行商发行,其技术水平也良莠不齐,插件程序很可能与其他运行中的程序发生冲突,从而出现各种页面错误、运行时间错误等现象,影响了正常的网页浏览。

对于安全要求较高的用户来说,可以通过以下方式加强对 Web 浏览器插件的防范(以 IE 为例)。

(1) 在位于网络边界的防火墙,通过安全配置,限制文件类型为 .ocx、.dll、.cab 的文件通过防火墙进入内部网络。

(2) 屏蔽调用 nwscript.exe、cscript.exe、wscript.exe、regedt32.exe、regwiz.exe、regsvr32.exe、reg.exe、regini.exe 等程序的网页代码。

6.2.2 脚本的攻防

随着互联网应用的快速发展,各类脚本语言广泛应用到 Web 网站的开发中,在丰富了 Web 应用功能的同时,带来了安全风险和威胁。

1. 脚本语言

首先,通过脚本语言与高级语言之间的比较来说明脚本语言的功能特点。高级程序设计语言(如 C、C++ 等)是从最简单的计算机基本元素开始来构造数据结构和算法的,而脚本语言(如 Perl、VBScript 等)是以“粘贴”方式将系统已经存在的一组功能强大的构件连接起来。高级程序设计语言是一种强类型的用于复杂处理的语言,而脚本语言是一种无类型的只需在构件之间简单地建立连接,实现快速应用开发的工具语言。脚本语言与高级程序设计语言的另一个不同点是,脚本语言通常是被解释执行,而高级程序设计语言是编译执行。

简单地说,脚本语言由一组文本形式的命令组成,脚本程序在执行时是由系统中的解释器将其逐条翻译成机器可识别的指令,并按程序顺序执行。正因为脚本程序在执行时多了一个翻译的过程,所以它要比高级程序设计语言开发的二进制程序的执行效率要低。

脚本(Script)通常可以由应用程序临时调用并执行。各类脚本被广泛地应用于 Web 网页设计中,因为脚本不仅可以减小网页的规模和提高网页浏览速度,而且可以丰富网页的显示方式(如动画、声音等)。例如,为了方便联系,一些单位喜欢在单位网站的显眼位置显示单位或领导邮箱的链接,当用户单击网页上的邮箱地址时会自动调用本地计算机上的电子邮件客户端软件(如 Outlook Express、Foxmail 等),这一功能就是通过脚本来实现的。

目前使用的脚本语言较多(如 JavaScript、VBScript、ActionScript、MAX Script、ASP、JSP、PHP、SQL、Perl、Shell 等),但脚本语言的执行一般只与相应的解释器有关,所以只要系统中存在相应语言的解释器程序就可以运行对应的脚本程序。

2. 脚本的攻防

也正是因为脚本具有语法和结构较为简单、脚本程序编写容易及不需要事先编译等特点,往往被攻击者利用。例如,在脚本中加入一些破坏计算机系统的命令,这样当用户浏览网页时,一旦调用这类脚本,便会使用户的系统受到攻击。

用户可以根据对所访问网页的信任程度选择安全等级,特别是对于那些信任度较低的网页,更不要轻易允许使用脚本。以 IE 浏览器为例,可通过“安全设置”对话框,禁用“脚本”选项下的部分功能,如图 6-4 所示。



图 6-4 管理 IE 浏览器中的脚本

3. 脚本病毒及防范方法

脚本病毒是计算机病毒的一种新形式,主要采用脚本语言编写,它可以对系统进行操作,包括创建、修改、删除,甚至格式化硬盘,具有传播速度快、危害性大等特点。借助脚本语言的特点,脚本病毒的编写形式灵活,容易产生变种。目前网络上存在的脚本病毒绝大多数都用 VBScript 或 JavaScript 编写。

脚本病毒的检测与防范思路与对传统病毒的检测与防范方法基本相同。传统的病毒检测方法包括特征代码法、校验和法、行为监测法、软件模拟法等。特征代码法提取病毒的某一小段特征代码进行识别,所以对未知病毒几乎无法预测,另外在新增病毒的数量不断加大的情况下,病毒特征代码的数量也在加大,会影响检测速度;校验和法是对文件作校验和,并将其保存,一旦校验和改变,就视为异常,这种检测方法依赖文件长度和内容,预警过于敏感,容易产生误报;行为监测法从理论上讲可以监测到未知病毒,但是实现复杂,速度较低。

6.3 针对 Web 浏览器 Cookie 的攻防

Cookie 是用来在服务器上存放用户信息的小文件。Cookie 的提出是为了解决 HTTP 协议的无状态性,使得 HTTP 协议可以识别上网的用户。但是,这一功能的实现却为网络攻击提供了一条便捷的通道。

6.3.1 Cookie 介绍

Web 应用的实现基础是应用层协议 HTTP,而 HTTP 本身是一种无状态(stateless)、面向非连接的协议,采用 HTTP 无法实现 Web 站点之间的交互。为弥补 HTTP 存在的不足,推出了 Cookie 这一状态管理机制。Cookie 是对 HTTP 功能的扩展,可以实现对 Web 客户端与 Web 服务器端连接状态的管理。Cookie 一经推出便引起了用户的普遍关注,目前已广泛应用于用户身份认证、网上购物、广告投放、定制用户喜欢的页面等网络活动中。例如,当用户进行网购时,一般一个用户需要同时购买多个商品,所以服务器需要记住用户的身份,在完成所有物品选购(放入“购物车”)后统一进行结算。

Cookie 技术最先被 Netscape 公司引入到 Navigator 浏览器中。之后,World Wide Web 协会支持并采纳了 Cookie 标准,微软公司也在其浏览器 Internet Explorer 中使用了 Cookie。现在,绝大多数浏览器都支持 Cookie 或兼容 Cookie 机制的使用。根据 Netscape 的定义,Cookie 是指在 HTTP 协议下,服务器或脚本可以维护客户端计算机上信息的一种方式。具体来讲,Cookie 是用户在浏览 Web 站点时,由 Web 服务器的 CGI(Common Gateway Interface)、ASP(Active Server Pages)等脚本创建并发送给浏览器的体积很小的纯文本信息,在 Web 浏览器未关闭之前它保存在客户端计算机的内存中(此种 Cookie 称为 session Cookie),当 Web 浏览器关闭后可作为文件保存在客户端的硬盘中(此种 Cookie 称为 persistent Cookie)。当创建了 Cookie 后,只要在其有效期内,当用户访问同一个 Web 服务器时浏览器首先要检查本地的 Cookie,并将其原样发送给服务器。这种状态信息称为“persistent client state http cookie”,简称为 Cookie。

Cookie 的工作机制为:当某一用户浏览某个使用 Cookie 的网站时,该网站的服务器就会为该用户产生一个唯一的标识符,并以此作为索引在服务器的后端数据中产生一个项目。接着,在给该用户的 HTTP 响应报文中添加一个称为 Set cookie 的首部行,首部字段名为“Set cookie”,其“值”为服务器为该用户生成的标识符。下面是一个首部行:

```
Set - cookie: cdniid5dd45dfdfddd
```

当该用户收到这个响应时,所使用的浏览器就在它管理的 Cookie 文件中添加一行,其中包括分配标识符的服务器的主机名和 Set cookie 后面给出的标识符。当该用户继续浏览这个网站时,每发送一个 HTTP 请求报文,其浏览器就会从其 Cookie 文件中取出这个网站的标识符,并放到 HTTP 请求报文的 Cookie 首部行中,内容形式如下:

```
Cookie: cdniid5dd45dfdfddd
```

于是,这个网站就能够跟踪该用户(其标识符为:cdniid5dd45dfdfddd)在该网站上的活动,并以时间先后顺序进行记录。这时,如果该用户所访问的是一个购物网站,服务器就会记录并维护一个购物列表,供用户最后进行结算。

如果该用户在一段时间内再次访问该网站,其浏览器会在 HTTP 请求报文中继续使用首部行“Cookie: cdniid5dd45dfdfddd”,服务器在收到该请求报文后,会根据该用户之前浏

览网站的行为,为其推荐相关的商品。如果该用户在该网站上使用过信用卡支付,该网站服务器也会记录并保存该用户的姓名、信用卡号码、联系方式等信息。这样,当该用户在该网站上购物时,只要使用了相同的计算机,由于浏览器产生的 HTTP 请求报文中包含的 Cookie 首部行与之前的相同,服务器就可以利用 Cookie 来识别出用户,以后该用户访问该网站时就不再要求输入用户名、密码等信息,从而实现了一次认证多次登录的功能。

6.3.2 Cookie 的组成及工作原理

存储在硬盘中的 Cookie 文件格式为:用户名@网站地址[数字].txt,如 abc@mail.jspi[2].txt。Cookie 文件的存放位置与操作系统和浏览器相关,这些文件在 Windows 操作系统中称为 Cookie 文件,在 Macintosh 操作系统中称为 Magic Cookie 文件。在 Windows XP 操作系统中,Cookie 文件存放在 C:\Documents and Settings\用户名称(用户登录账号)\Cookie 文件夹下。

1. 由 Web 服务器端生成的 Set-Cookie 格式

服务器生成的 Cookie 称为 Set-Cookie Header,其内容由“名称值”对(name-value pairs)组成,其基本格式如下:

```
NAME = VALUE; Expires = DATE; Path = PATH; Domain = DOMAIN_NAME; Secure
```

其中,不同的项之间以“;”分开,在所有的项中,除了第一项 NAME=VALUE 是必选项外,其他部分均为可选项。每一项的说明如下。

(1) NAME=VALUE。该项是每一个 Cookie 都必须有的组成部分。其中,NAME 是该 Cookie 的名称,VALUE 是该名称的值。需要注意的是,在 NAME=VALUE 项中不含分号、逗号和空格等字符。

(2) Expires=DATE。该选项是一个只写变量,它确定了 Cookie 时间的有效期。其书写格式为:星期几,DD-MM YY HH:MM:SS GMT(其中,GMT 表示格林威治时间)。

需要强调的是:该变量可以省略。如果省略该变量时,则 Cookie 的属性值不会保存在用户的硬盘(称作 persistent Cookie)中,而是保存在内存(称为 session Cookie)中,Cookie 信息将随着浏览器的关闭而自动消失。

(3) Domain=DOMAIN_NAME。Domain 是指该 Cookie 所在的主机名或域名,一般为域名。Domain 确定了哪些 Intranet 或 Internet 域中的 Web 服务器可读取客户端 Web 浏览器中所存取的 Cookie 信息。该选项是可选的,默认时系统自动设置 Cookie 的属性值为该 Web 服务器的域名。

(4) Path=PATH。Path 定义了 Web 服务器上能够获取 Cookie 的路径,即 Web 服务器上的哪些页面可获取服务器设置并创建 Cookie。如果 Path 属性的值为“/”,则该 Web 服务器上所有的 WWW 资源均可读取该 Cookie。该选项的设置是可选的。默认时,Path 的属性值为 Web 服务器传给浏览器的资源的路径名。通过对 Domain 和 Path 这两个变量的有机结合,可有效地控制 Cookie 文件被访问的范围。

(5) Secure。当 Cookie 中存在该变量时,表明只有当浏览器和 Web 服务器之间的通信

协议为加密认证协议时浏览器才向服务器提交相应的 Cookie。目前所采用的安全加密协议一般为 SSL/TLS。

在具体操作中,一个 HTTP 响应报文中可以同时发送多个 Set-Cookie 信息。例如, CGI 程序通过调用 GetCookie() 函数读取 HTTP 报头中的 Cookie,通过调用 SetCookie() 函数对 HTTP 报头中的 Cookie 进行设置。

2. 由 Web 客户端生成的 Cookie 格式

由客户端生成的 Cookie Header 由“NAME=VALUE”对组成,其格式为:

```
NAME1 = VALUE1[;NAME2 = VALUE2] ... [;NAMEi = VALUEi]
```

其中,NAME_i 表示第 *i* 个 Cookie 的名称,VALUE_i 表示其值。这里的 NAME 和对应的 VALUE 与 Set-Cookie 中的相同。

Web 客户端可以通过 VBScript、JavaScript 等脚本程序来对 HTTP 报文中的 Cookie 进行读写操作。例如,在 ASP 中,Cookie 是附属 Response 对象和 Request 对象的数据集合,使用时只需要在前面加上 Response 和 Request 即可。

Cookie 机制对 Web 客户端存放的 Cookie 在数量和文件大小上都进行了限制。其中,每一个 Web 客户端存放的 Cookie 数量不超过 300 个,每一个 Cookie 不超过 4KB,针对每一个域名最多保存 20 个 Cookie。

3. Cookie 的工作原理

Cookie 使用 HTTP 头部(Header)来传递和交换信息。Cookie 机制定义了两种 HTTP 的报文头部: Set Cookie Header 和 Cookie Header。其中,Set Cookie Header 存放在 Web 服务器站点的响应头部(Response Header)中,当用户通过 Web 浏览器首次打开 Web 服务器的某一站点时,Web 服务器先根据用户端的信息创建一个 Set Cookie Header,并添加到 HTTP 响应报文中发送给 Web 客户端; Cookie Header 存放在 Web 客户端的请求头部(Request Header)中,当用户通过 Web 浏览器再次访问 Web 服务器的站点(其实是 Web 页面)时,Web 浏览器根据要访问的 Web 站点的 URL 从客户端的计算机中取回 Cookie,并添加到 HTTP 请求报文中发送给 Web 服务器。Cookie 的工作过程如图 6-5 所示,具体描述如下。



图 6-5 Cookie 的工作过程

(1) Web 客户端通过浏览器向 Web 服务器发起连接请求,通过 HTTP 报文请求行中的 URL 打开某一 Web 页面。

(2) Web 服务器接收到请求后,根据用户端提供的信息产生一个 Set-Cookie Header。

(3) 将生成的 Set-Cookie Header 通过 Response Header 存放在 HTTP 报文中回传给 Web 客户端,建立一次会话连接。

(4) Web 客户端收到 HTTP 应答报文后,如果要继续已建立的这次会话,则将 Cookie 的内容从 HTTP 报文中取出,形成一个 Cookie 文本文件储存在客户端计算机的硬盘中或保存在客户端计算机的内存中。

(5) 当 Web 客户端再次向 Web 服务器发起连接请求时,Web 浏览器首先根据要访问站点的 URL 在本地计算机中寻找对应的 Cookie 文本文件或在本地计算机的内存中寻找对应的 Cookie 内容。如果找到,则将此 Cookie 内容存放在 HTTP 请求报文中发给 Web 服务器。

(6) Web 服务器接收到包含 Cookie 内容的 HTTP 请求后,检索其 Cookie 中与用户有关的信息,并根据检索结果生成一个客户端所请求的页面应答传递给客户端。

Web 浏览器的每一次页面请求(如打开新页面、刷新已打开的页面等),都会与 Web 服务器之间进行 Cookie 信息的交换。

6.3.3 Cookie 的安全防范

尽管 Cookie 能够简化用户访问授权网站时的操作过程,不需要在每次访问网站时都输入登录信息,使用户的上网过程更加便捷。但是,Cookie 的使用为网络安全带来了隐患,主要是 Cookie 的存在泄露了用户信息。例如,当网站服务器在记录了用户的上网信息后,就可能会将这些信息提交给地下黑色产业链以牟取更大的经济利益。

其中,在 Set Cookie 内容的组成中,只有 NAME 项是必备的,而 Expires、Path、Domain、Secure 等项是可选的。对 Cookie 内容可选项的灵活应用,可以使 Cookie 适用于各种不同的应用环境,满足不同条件下用户的需求。例如,通过 Path 值的设置可以限制 Cookie 在服务器上的访问路径,通过对 Expires 值的设置可以让 Web 浏览器将 Cookie 是否写入本机的硬盘或设置 Cookie 的有效期,通过对 Secure 项的设置决定 Cookie 在传输中是否采用加密方式等。对于 Cookie 的这些可选项,开发人员在使用时必须注意其安全性设置,否则将会存在安全隐患,导致各类安全问题的发生。

1. Cookie 域的安全防范

域(Domain)是 Set Cookie 的可选项,用于确定哪一个 Web 服务器上的站点能够访问 Cookie 中的信息。如果该项为空,则产生该 Cookie 的 Web 服务器上的所有站点都会访问 Cookie 中的信息。为了仅让 Web 服务器上的指定站点能够访问对应 Cookie 中的信息,Cookie 中的域值不能为空。

Cookie 的另一个特点是允许对所有匹配域名的 Web 站点进行访问,如果将域值设置为 jspt. cn,那么根据域名自右向左的匹配原则,所有像 lib. jspt. cn、media. jspt. cn、str. pic. top. jspt. cn 等凡符合 *. jspt. cn 的域名都匹配 jspt. cn。如图 6.6 所示,假设在域名 jspt. cn 上分别创建了 lib. jspt. cn 和 media. jspt. cn 两个 Web 站点,其可能出现的安全问题描述如下。

(1) 用户首先访问 lib. jspt. cn 对应的 Web 站点。

(2) lib. jspt. cn 站点创建了一个如下的 Set-Cookie。

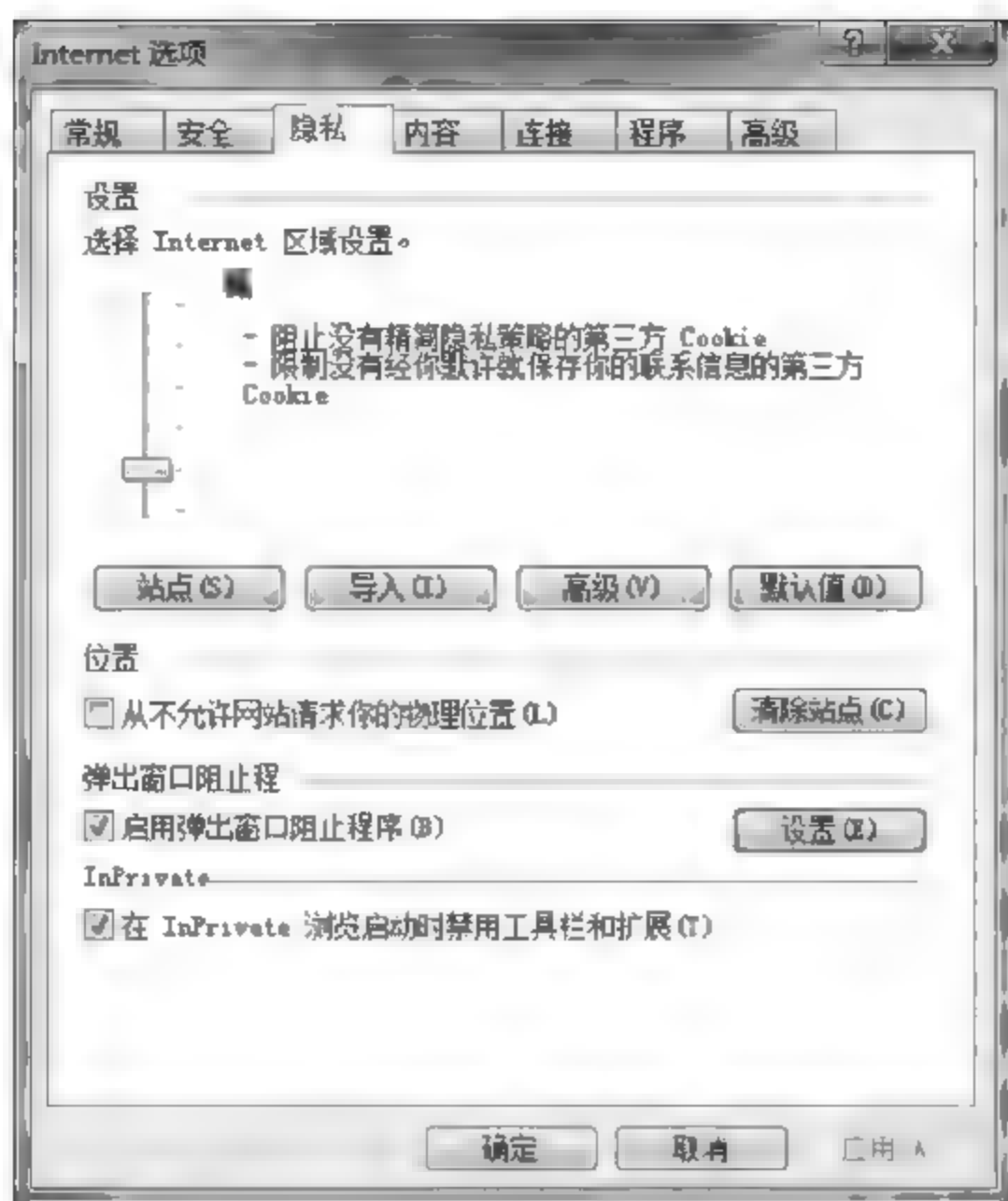


图 6-7 设置是否或在什么程度上接收 Cookie

6.4 网页木马的攻防

随着 Web 浏览器的发展,其功能不断丰富,但安全威胁越来越突出。其中,自从在 Web 浏览器中引入了 JavaApplet、VBScript、JavaScript 等客户端执行脚本语言之后,这些脚本代码可以在浏览器端执行,以此丰富了浏览器的功能。与此同时,攻击者利用浏览器所具有的这一机制编写一些攻击脚本,来对 Web 客户端实施攻击。如果这些攻击脚本再利用客户端软件存在的安全漏洞获取到对客户端计算机的访问权限,存在的安全威胁将会更加严重。网页木马就是通过在浏览器中植入木马程序从而实现对 Web 客户端进行攻击的一项技术。

本节在第 4 章有关木马和网页木马相关知识的基础上,从攻防角度继续介绍网页木马的相关内容。

6.4.1 网页木马的攻击原理

早期的网络攻击对象主要针对的是操作系统和网络服务。近年来,一方面由于 Web 应用得到快速发展,原来大量的基于传统 C/S 模式的应用逐渐迁移到了 B/S 模式,Web 浏览器成为客户端应用软件的主流;另一方面由于防火墙、入侵检测和入侵防御等安全系统的部署,针对网络服务器的攻击难度逐渐加大。在此情况下,利用 Web 浏览器存在的安全漏洞的攻击行为更加普遍。

自动加载。

由于 Web 实现技术的多样性,基于内嵌链接方式的网页挂马实现方法较多,最常见的有以下3种。

1) 内嵌 HTML 标签

HTML 标签是 HTML 语言中最基本的单位,主要格式如下:

```
<html>
  <head>
    * 文档的头部,...
    ...
  </head>
  <body>
    * 文档的主体,...
    ...
  </body>
</html>
```

在内嵌 HTML 标签中,frame 和 iframe 的应用具有特殊性,都可以在一个 HTML 文档中嵌入另一个 HTML 文档,例如(以 iframe 为例):

```
<html>
  <head></head>
  <body>
    <iframe src = "abc.html"></iframe>
  </body>
</html>
```

利用此功能,攻击者可以将网页木马链接嵌入到网站首页或其他页面中。为了更好地隐蔽被嵌入的网页木马,攻击者一般会利用层次嵌套的内嵌标签,引入一些中间的跳转站点并进行混淆,为网页木马的检测和追踪增加难度。

由于在 HTML5 中不再支持<frame>标签,因此目前内嵌标签中大量使用 iframe。iframe 的功能是在页面中创建一个内嵌框架(框架便是将网页画面分成几个窗口,每个窗口对应一个 URL,利用框架可以在一个页面中同时访问多个 URL),用于包含和显示其他 HTML 文档的内容,当在浏览器中打开包含内嵌框架的 HTML 页面时,被包含在内嵌框架中的 URL 也会在各自的框架中被自动打开。攻击者利用<iframe>标签的这一特征,可以直接或间接地嵌入网页木马,并将标签的 width 和 height 属性设置为 0(不可见)来避免被挂马的页面在视觉效果上发生变化。例如:

```
<iframe src = "abc.html" width = "0" height = "0" frameborder = "0"> </iframe>
```

其中,abc.html 为被挂木马页面的 URL。

2) 内嵌对象链接

内嵌对象链接是利用 Flash 等工具内嵌对象中的特定功能来实现指定页面加载的一种方法。例如,利用 Flash 脚本中的 LoadMovie() 函数可以动态地从外部加载 SWF、JPG 等

图片文件,从而减少主文件的大小,有利于快速浏览,还可以对被加载的图片文件根据需要进行修改或更换。这样,只需要把主文件和待加载的图片文件上传到指定的空间,就可以方便地实现只下载主文件,如果需要浏览图片文件时再单独下载,以提高网页浏览的效率,提升用户的体验。

如果整个 Flash 网页不分主次,全部集中在一个达到几兆字节大小的 Flash 文件中,即使内容再好的页面,谁还有耐心等着看呢! 使用 LoadMovie() 函数可以将外部 SWF 文件载入到某一层上,或将外部 SWF 文件载入到时间轴的某个影片剪辑中。基于此功能,攻击者可以编写一些包含网页木马链接的 SWF 或 JGP 等文件,再将其作为被 LoadMovie() 函数加载的外部文件,从而实现挂马攻击。

3) 恶意 Script 脚本

利用 Script 脚本标签通过外部引用脚本的方式来实现网页木马是网页挂马中最常用的一种方法。例如, <script src="URL to abc.html">, 其中 abc.html 为被挂木马页面的 URL。另外,跳转脚本通常使用 document.write 动态生成包含网页木马链接的 iframe 内嵌标签,或使用 window.open() 函数弹出一个新 HTML 窗口链接网页木马进行攻击。例如:

```
<html>
  <head>
    <script type="text/javascript">
      function open_win()
      {
        window.open("http://www.abc.com.cn")
      }
    </script>
  </head>
  <body>
    <input type="button" value="Open Window" onclick="open_win()" />
  </body>
</html>
```

可以在新浏览器窗口中打开 www.abc.com.cn, 如果 www.abc.com.cn 是一个网页木马, 就可以在新浏览器窗口弹出的过程中进行攻击。

2. 网页动态视图

网页动态视图是指浏览器处理被访问页面时所加载的所有内嵌页面、内嵌脚本的层次关系图。在传统的针对 Web 服务器的攻击中, 攻击者通常利用网站服务器的漏洞获得相应权限来篡改页面、嵌入攻击脚本或攻击页面, 但这种方式很难适用于那些安全防御比较严密的站点。

由于浏览器在访问页面时会加载其整个动态视图, 攻击者可将攻击脚本或攻击页面挂载到页面动态视图中的任意位置来进行网页挂马。在第三方流量统计、广告位等处嵌入攻击脚本或攻击页面, 是攻击者对一些门户网站页面进行挂马的常用手段。如图 6-8 所示, 网站 C 的一个提供流量统计服务的页面是网站 A 的首页动态视图的一部分, 攻击者通过 <iframe> 标签将攻击页面挂载到这个流量统计页面中(图 6-8 中的虚线箭头)。如果网站

A 的首页被挂马,由于内嵌链接的自动加载存在递归性(即内嵌页面中的内嵌链接也会被自动加载),客户端在访问网站 A 的首页时会自动加载流量统计页面,随后也会加载流量统计页面中嵌入的攻击页面。

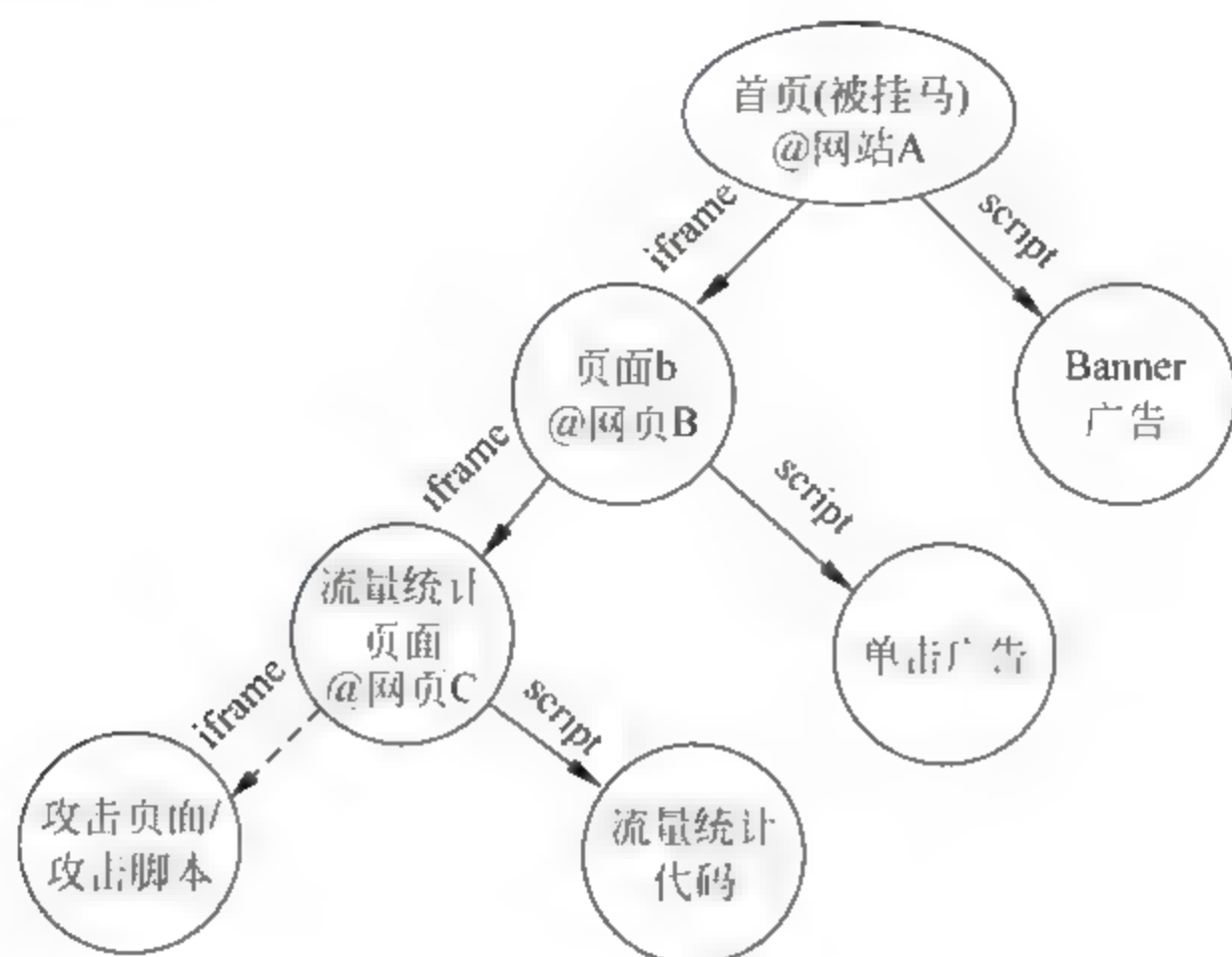


图 6-8 基于网页动态视图的木马感染途径

虽然网页挂马是对网站服务器中的页面进行篡改,但攻击者进行网页挂马的目的在于攻击客户端,浏览器在访问被挂马页面时,依照感染链将攻击脚本或攻击页面加载到客户端,最终让客户端自动下载、执行恶意程序。

网页挂马已经成为攻击者在部署网页木马时普遍采用的手段。一方面,与通过社会工程学手段诱使用户直接访问攻击页面相比,网页挂马使客户端在访问被挂马页面时按照网页木马感染途径自动加载攻击脚本或攻击页面,有更好的隐蔽性;另一方面,攻击者通过一定的挂马策略可以很好地保证攻击脚本或攻击页面在客户端的加载量。例如,对热点事件有关页面进行挂马,对门户网站首页等访问量大的页面进行挂马等。

6.4.3 网页木马关键技术

网页木马以页面为攻击对象,是一种基于 Web 的客户端攻击方式。从恶意代码的特征来分析,网页木马是一种新形态的恶意代码,其组成和结构与蠕虫、计算机病毒等恶意代码有很大区别。在这种新的攻击形态中,攻击者经常使用一些灵活多变的技术和手段来提高网页木马攻击的成功率,并可以躲避防御方的检测与反制。

1. 提高网页木马攻击性的技术

网页挂马虽然使客户端访问被挂马页面时自动加载攻击脚本或攻击页面,但却无法保证攻击脚本或攻击页面被客户端加载后一定能攻击成功。这是因为:一方面,攻击页面或攻击脚本针对的漏洞一般只存在于特定版本的浏览器和插件中,而客户端浏览环境各异,如果攻击对象与客户端浏览环境不匹配,就会导致攻击失败;另一方面,即使客户端浏览环境中存在相关漏洞,但操作系统防御技术的不断升级,使得该漏洞被成功利用变得更加困难。

在攻击过程中,攻击者为了应对客户端浏览环境的多样性,需要采用一种 all-in-one(一体化)的方式将针对不同漏洞的攻击代码全部包含在单个攻击页面中。但这种方式导致大

性,就必须在代理处有效检测出被挂马页面并阻止客户端浏览器加载该页面的同时,也不能使客户端在用户体验上有明显差别。也就是说,代理技术的存在对用户来说是透明的。

3. 客户端网页木马的防范方法

从技术上讲,客户端网页木马的防范可以采用以下方法来实现。

(1) 设置 URL 黑名单。以 Google 搜索引擎的安全应用为例,Google 将基于页面静态特征进行机器学习的检测方法与基于行为特征的检测方法相结合,对其索引库中的页面进行检测,生成一个被挂马网页的 URL 黑名单,Google 搜索引擎会对包含在 URL 黑名单中的搜索结果做标识。

基于 URL 黑名单过滤的最大问题在于时间上的非实时性以及范围上的不全面性。挂马页面的数量存在快速增加的态势,虽然 Google 周期性地检测页面,但一个页面很可能在被 Google 判定为良性之后又被挂马,用户随后浏览该页面时就可能遭到攻击。尽管 Google 爬取了大量页面并对其进行检测,但仍无法保证 100% 的覆盖面。

(2) 浏览器安全加固。目前,浏览器安全加固主要通过通过在浏览器中增加网页木马检测,以及已知漏洞利用特征检测等功能来实现浏览器应用的安全性。不同类型的浏览器实现安全加固的方法不尽相同,读者可参阅相关浏览器的安全加固技术说明。

(3) 操作系统安全扩展。由于存在大量的漏洞,因此浏览器是一个不安全的 application 环境。但是,与浏览器相比较,客户端的操作系统是一个相对安全的环境。一般可通过对操作系统做一定的安全扩展,来阻断网页木马攻击流程中未经用户授权的恶意可执行文件下载、安装或执行。例如,通过采用虚拟隔离存储空间技术,任何通过浏览器进程下载的可执行文件都被放入一个虚拟的、权限受限的隔离存储空间,只有经过用户确认的下载文件才会被转移到真实的文件系统中。这种方法在一定程度上阻断了恶意可执行文件在客户端的下载和执行。

除以上介绍的基本技术之外,客户端网页木马防范的有效途径是提升客户端操作系统和浏览器的安全性,具体方法是采用操作系统本身提供的在线更新功能,以及第三方软件所提供的对常用软件的更新机制,来确保所使用的 Web 客户端计算机始终处于一种相对安全的状态。与此同时,安装一款功能较强的反病毒软件并对其进行实时更新,是应对网页木马威胁必不可少的一个环节。另外,还要养成良好的上网习惯。

6.5 网络钓鱼的攻防

人们日常生活中对“钓鱼”一词理解为一种欺诈行为。钓鱼网站可简单地理解为不法分子为了实施网络攻击精心构建的具有欺诈性的特殊类型的网站,利用钓鱼网站实施的 network 攻击称为网络钓鱼攻击。

6.5.1 网络钓鱼的概念和特点

网络钓鱼(phishing)由钓鱼(fishing)一词演变而来。在网络钓鱼的过程中,攻击者将诱饵(如电子邮件、手机短信、QQ 链接等)发送给大量用户,期待少数安全意识弱的用户“上钩”,进而达到“钓鱼”(如窃取用户的隐私信息)的目的。

随着移动互联网的迅猛发展,无线接入网络承载的业务已经由原来的单一语音,转变到现在的综合语音、数据和图像的多媒体应用,无论是移动性、带宽、实时性、覆盖范围,还是可管理性和可融合性,原有接入网络已经无法满足其需求。目前,4G网络的全面推广似乎解决了移动互联网中存在的一些问题,但信号覆盖范围、数据业务与语音业务的融合等关键问题还没有很好地解决,等到5G到来后,这些问题是不是会全部解决,仍然还是一个未知数。同时,任何一项新应用的出现,同时也会伴随着新安全问题的产生。

7.1.4 应用服务

网络的核心是应用,网络中其他技术都是为应用而服务的。与传统的互联网应用相比,移动互联网的应用必须支持可移动性和内容的可定制性,尤其提供的内容要视不同的社会群体需要能够自由选择和定制。目前,主要的应用服务包括移动搜索、移动社交网络、移动电子商务、基于智能手机的定位服务等。

1. 移动搜索

百度、Google等传统的互联网搜索服务为传统互联网应用带来了极大的便利,为人们获取知识、寻求帮助、促进交流提供了途径,加速了互联网应用的发展。移动搜索以移动互联网应用为特点,提出了比传统搜索服务更多的需求。

移动搜索是指基于移动网络的搜索技术,具体是指用户通过智能手机、PDA、平板电脑等移动终端设备,利用浏览器、短信、交互式语音应答(Interactive Voice Response, IVR)等多种搜索方式,获取所需的信息和服务。

虽然移动搜索是对传统互联网搜索服务的扩展,但移动搜索在用户操作的便捷性、搜索结果的显示方式以及个性化服务等方面都表现出了不同以往的要求。例如,由于手机等移动终端在屏幕显示、输入方式、网络带宽、电能等方面都受到了限制,因此移动搜索的显示结果在能够正确表述内容的前提下应尽可能简约,力求一目了然。也可以采用分级显示的方式,根据用户选择,从简到繁逐级显示。

2. 移动社交网络

社交网络服务(Social Networking Services, SNS)是指为一群拥有相同兴趣或存在社会关系的人创建的在线社区。这类服务往往是基于互联网,为用户提供各种联系、交流的交互通路,如电子邮件、即时通信服务(如QQ、MSN)等。

SNS源自网络社交,从网络出现开始,人们之间便通过电子邮件实现点对点的信息发送,随后出现的BBS实现了一对多点的信息发布,BBS把网络社交向前推进了一步。即时通信(IM)和博客(Blog)更像是前面两个社交工具的升级版本,IM提高了即时效果(传输速度)和同时交流能力(并行处理),而Blog则开始体现社会学和心理学的理论:信息发布节点开始体现越来越强的个体意识,因为在时间维度上的分散信息开始可以被聚合,进而成为信息发布节点的“形象”和“性格”。

随后的发展更是目不暇接,网络社交衍生出了社交网络,从Facebook、Twitter、YouTube,到人人、微博、优酷,从以前的短信拜年,到现在越来越多的微信祝福。由此可以这样来描述移动社交网络:它并不是新生事物,更像是社交网络服务与移动终端特性的自然结合。简单地说,就是用户将进行网络社交活动的媒介,更多地从传统的Web网页转移

到了移动 APP(application 的缩写)上。而这个看似简单的转移,却包含了不小的意义,即从社交网络服务形成初期,人们逐渐将线下生活的更完整的信息流转移到线上进行低成本管理,从而发展为大规模的虚拟社交,到现在通过移动终端更紧密地结合了现实生活的各种元素,形成虚拟社会与真实社会的更深层的交织。

3. 自媒体

在由谢因波曼与克里斯威理斯两位学者联合提出的“*We Media*”(自媒体)研究报告中,对自媒体进行了较为严谨的定义:“自媒体是普通大众经由数字科技强化与全球知识体系相连之后,一种开始理解普通大众如何提供与分享他们自身的事实、新闻的途径。”根据这一定义,可以将自媒体理解为:普通大众用以发布自己亲眼所见、亲耳所闻事件的载体,这些载体包括博客、微博、微信、论坛/BBS 和个人门户等网络社区。自媒体是一种“公民媒体”或“个人媒体”,它的特点是私人化、平民化、泛在化和自主化。

在自媒体时代,原有的“主流媒体”不再是社会声音的唯一来源,也不再是“统一的声音”,普通大众都可能成为信息的生产者、传播者和分享者。传统的新闻媒体在传播者与受众之间存在一条很明晰的界线,是一种“自上而下”的“点到面”的传播方式,而自媒体打破了这一格局,通过“点到点”或“点到多点”的传播方式,每个人既是媒体的传播者也是新闻提供者。各种形式的自媒体使得原来处于新闻制造边缘的受众成为新闻信息传播的中坚力量,传统媒体受到自媒体的挑战。目前,自媒体平台主要有美国的 Facebook 和 Twitter,中国的 QQ 空间、新浪微博、腾讯微博、微信朋友圈、微信公众平台、人人网、百度贴吧、皮皮精灵等。

7.1.5 安全与隐私保护

安全是一个永恒的命题。移动互联网不仅要解决传统互联网中存在的安全问题,而且还要不断面对新环境中出现的新的安全问题。对于任何一种网络类型或应用来说,如果安全问题解决不好,必然会影响甚至是阻碍其应用的发展。

在图 7-1 所示的移动互联网体系结构中,每一个层面都会涉及安全问题,而且任何一个安全问题的出现,都会影响到整个移动互联网的应用。下面,通过移动终端的安全和定位信息安全两个实例,分析移动互联网存在的安全问题和隐私保护问题。

1. 移动终端的安全

与传统互联网中的服务器和个人计算机相比,移动互联网中的移动终端在安全技术的实施上存在以下困难或不足。

(1) 移动终端的内存、CPU 处理能力和通信能力有限,所以一些在传统互联网中很成熟的安全方案在移动互联网中很难部署。例如,针对个人计算机的防病毒系统要求提供较大的存储空间来存放病毒库,但对手机等终端来说实现起来较为困难。

(2) 由于移动互联网的应用特点,许多恶意代码的传播更快,影响面更广,造成的威胁更大。

(3) 手机需要长时间处于开机状态,这为黑客的攻击提供了更大的可能性和更高的成功率。

(4) 手机等移动终端设备上一般都会保存联系人信息、照片等与设备拥有者相关的敏感信息,这些信息对黑客来说具有更大的吸引力,为此用户信息被窃取、监视和攻击的可能

性更大。

另外,目前国内大量终端都采用 Android 这一开源操作系统,其开放性在为 APP 开发提供便利的同时,同样也降低了攻击软件的编写和成功入侵的门槛。

2. 定位信息安全

定位是移动互联网中一项非常重要的应用。由于定位过程和结果都依赖于手机拥有者的个人信息,因此由定位而引起的隐私保护在移动互联网中将显得非常重要。定位涉及用户曾经去过哪里,正在做什么、将要去哪里,还有与谁在什么时间去哪里,正在与谁在一起等。这些问题都属于个人隐私保护的范畴,一旦被窃取和利用,将会对终端拥有者及相关人员造成很大的危害。为此,随着移动互联网应用范围的快速扩展,与位置相关的用户隐私保护引起社会普遍关注。

7.2 智能移动终端系统的攻防

智能移动终端是移动互联网中重要的组成部分。结合当前实际应用,本节主要以 Android 手机应用为基础,对 Android 操作系统及 APP 的主要安全问题进行介绍。

7.2.1 登录安全

当用户通过手机等终端进行网络支付等操作时首先要进行登录。在登录过程中,系统要求用户输入账号名称、密码以及用户的身份证号码等信息,之后再由客户端软件与服务器端进行通信,完成用户的上网行为。在这一过程中,一旦用户的登录过程被攻击者监视或劫持,通信数据被截获或破解,将会产生严重的安全问题。根据对各类安全事件的综合分析,目前较为严重的安全隐患主要有由加密机制引起的安全问题和由服务器证书验证产生的安全问题两个方面。

1. 加密机制的安全问题

加密机制安全问题是指因加密算法或方法不完整或过于简单,而被攻击者劫持和破解。数据加密是信息安全中采用最为广泛的一种方法,也是其他安全技术的基础和保障。目前,银行客户端等安全应用的登录加密机制一般采用 HTTPS 和“HTTP+数据加密”两种方式。其中,大部分安全客户端采用目前互联网通用的 HTTPS 加密机制,但也有部分安全客户端采用“HTTP+数据加密”机制。

(1) HTTPS 方式。HTTPS(HyperText Transfer Protocol over Secure Socket Layer, 基于安全套接字层的超文本传输协议),是以安全为目标的 HTTP 通道,是基于 HTTP 协议的安全版本。HTTPS 协议是在 HTTP 协议中加入 SSL 层,由 SSL 协议负责其安全性,用于安全的 HTTP 数据传输。HTTP 报文中信息是以明文方式传输的,而 HTTPS 则是通过具有安全加密机制的 SSL 加密方式进行传输。另外,HTTP 的连接方式很简单,是一种无状态的连接方式,而 HTTPS 协议是由 SSL+HTTP 协议构建的可进行加密传输、身份认证的网络协议。其连接的建立需要一套完善的交互机制的保障。

(2) “HTTP+数据加密”方式。“HTTP+数据加密”方式是指使用 HTTP 方式进行传

输,而采用加密机制对传输的数据进行加密处理。在该安全机制中,如果数据加密机制不完整或过于简单,就会存在安全风险。这里以一个实例说明该安全机制存在的问题,当采用“HTTP+数据加密”方式时,加密后的数据(密文)对 HTTP 协议来说是以“明文”来对待的,可以通过抓包软件,得到如图 7-3 所示的信息(注意:对于略懂计算机网络知识的人来说,是一件非常简单的事情)。这时,不管其中的内容是不是进行了加密,只需要原样进行复制后进行提交,就可以登录服务器,实现攻击目的。将这种攻击方式称为“重放攻击”。



图 7-3 抓包显示的 HTTP 协议中传输的信息

“重放攻击”(replay attacks)也称为新鲜性攻击(freshness attacks),即攻击者通过重放消息或消息片段达到对目标主机进行欺骗的攻击行为,主要用于破坏认证的正确性。重放攻击是攻击行为中危害较为严重的一种。例如,客户 C 通过签名授权银行 B 转账给客户 A,如果攻击者 P 窃听到该消息,并在稍后重放该消息,银行将认为客户 C 需要进行两次转账,从而使客户账户 C 遭受损失。

2. 服务器证书验证安全问题

服务器证书验证存在的安全问题是,当客户端登录服务器时,在通信过程中不对服务器端身份的合法性进行验证,从而导致登录过程容易被“中间人攻击”劫持。

如图 7-4 所示,中间人攻击(Man in-the-Middle Attack, MITM)是一种“间接”的入侵攻击方式,通过各种技术手段将受入侵者控制的一台计算机(或手机)虚拟放置在网络连接中的两台通信计算机之间,这台计算机就称为“中间人”(MIT)。然后入侵者把这台计算机模拟成一台或两台原始计算机,使“中间人”能够与原始计算机建立活动连接并允许其读取或修改传递的信息,然而两个原始计算机用户却认为他们是在互相进行直接通信。

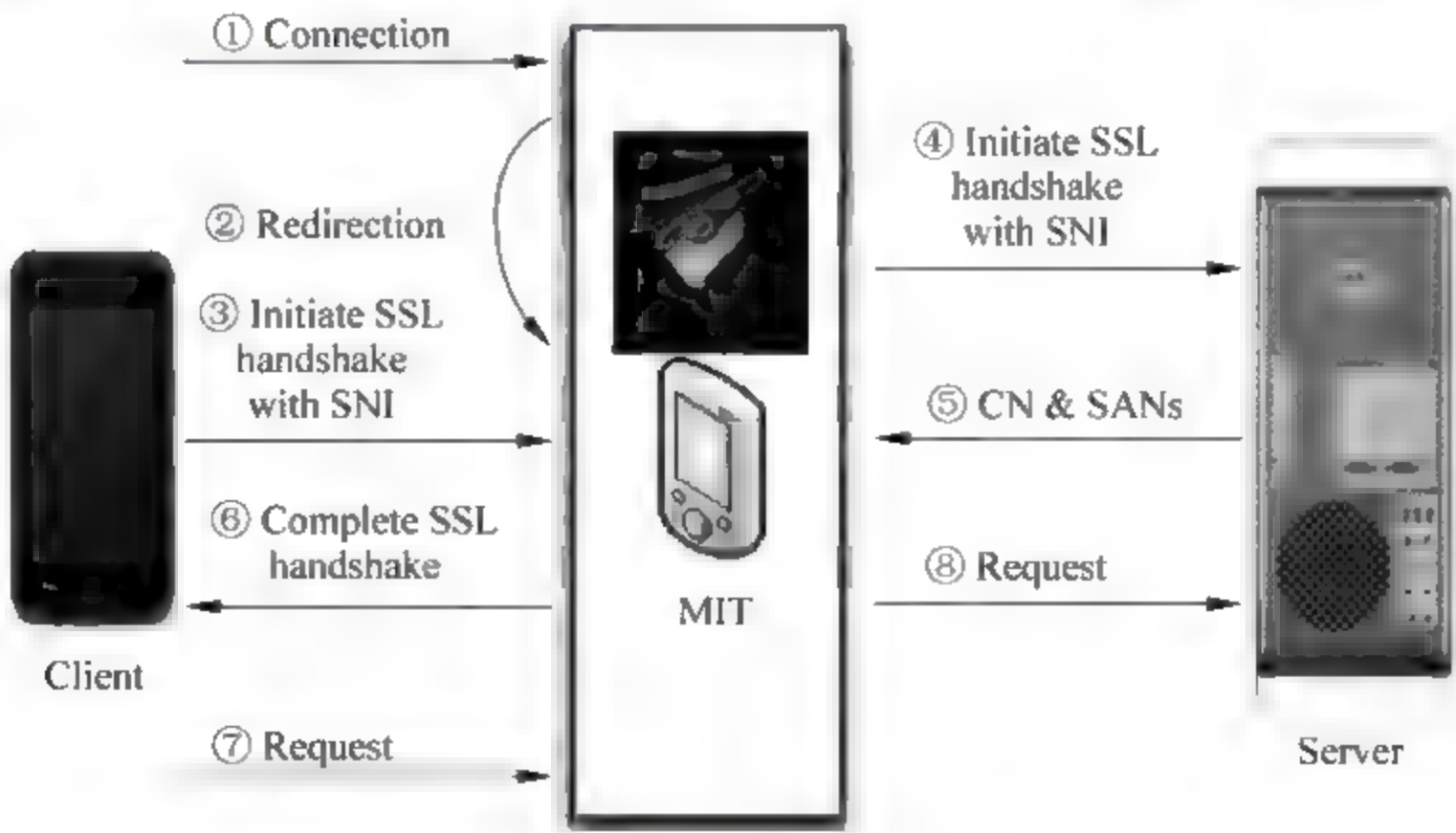


图 7-4 中间人攻击实现过程示意图

利用中间人攻击方式,攻击者可以冒充服务器与客户端进行通信,之后再冒充客户端与服务器进行通信,在充当中间人的过程中窃取了用户信息(如账号、密码等)。在图 7-4 所示

的中间人攻击中,由于客户端没有对服务器的证书进行验证(没有验证与其通信的服务器的身份),即客户端默认信任所有的服务器。利用这种信任,中间人中转了 HTTPS 中的 SSL 通信过程。这样一来,与客户端通信的并不是服务器而是中间人。中间人在知道了用于通信的密码后,就可以对 HTTPS 的通信数据进行窃听。其窃听过程为:中间人将自己的证书提供给客户端,而客户端在不进行验证的情况下,信任并使用此证书对要传输的数据进行加密,之后再传给中间人。

在以上攻击过程中,好像所有通信过程中的信息都是经过 HTTPS 协议加密的,但由于该密钥本来就是中间人与客户端之间“协商”而来的,因此中间人收到加密数据包后,就可以很方便地进行解密处理得到明文信息。对于用户来说,由于是与虚假的服务器进行通信,因此所有通信内容事实上全部可以被中间人获得。所以,像网上银行这些机构,如果不能严格地确定参与通信者的身份,那么任何加密手段的使用都没有意义。攻击者在窃取了通信数据后,便可以冒充合法用户进行登录,也可以制作钓鱼网站从事非法行为。中间人既欺骗了客户端,也欺骗了服务器。

针对服务器登录过程存在的安全威胁,最有效的解决办法是采用相对完善的 HTTPS 安全机制。

7.2.2 软键盘输入安全

软键盘是通过软件模拟传统计算机键盘的功能,通过鼠标单击或手指按压输入字符的一种软件。软键盘可以防止木马记录键盘输入的用户账户与密码等敏感信息,原来多用于银行网站上要求用户输入账号和密码的地方,现在几乎所有的移动终端设备都提供了软键盘功能。其实,Windows 操作系统早已提供了软键盘程序“Osk.exe”(图 7-5),具体位于 C:\Windows\system32 目录下。

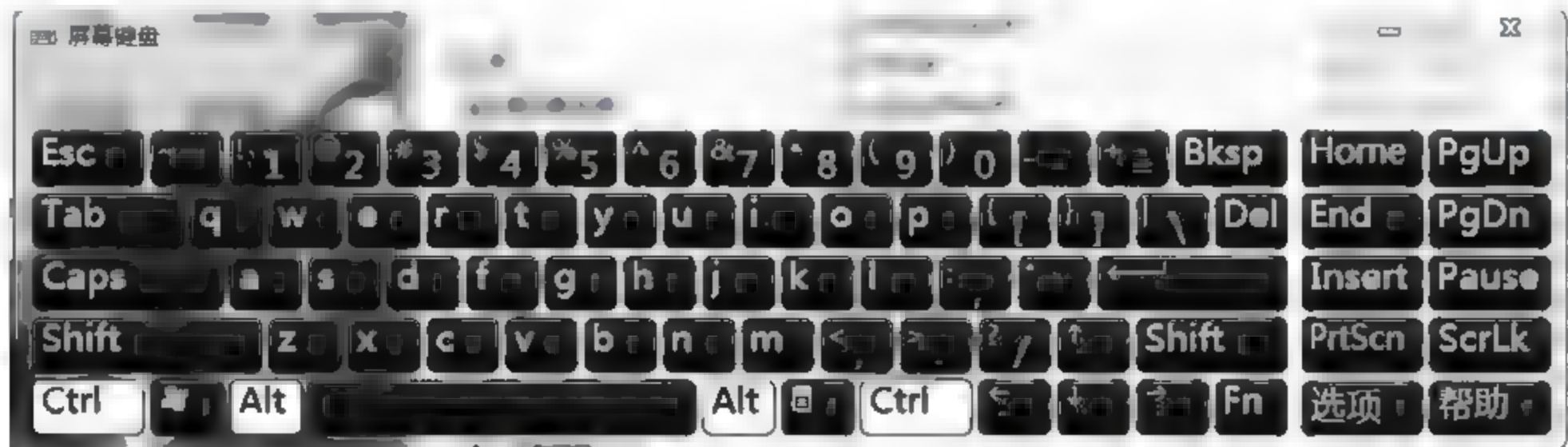


图 7-5 Windows 操作系统自带的软键盘

1. 软键盘输入方式

借鉴台式计算机上通过强制用户安装安全插件后才能显示输入框这一安全保护措施,手机等智能移动终端设备在客户端软件的信息输入框处定制了一套自己的输入方式,即通过软键盘输入来防止恶意输入法等应用软件窃取用户信息。

移动终端上采取的软键盘一般分为 3 种类型:系统默认输入法、自绘固定软键盘和自绘随机软键盘。其中,使用系统默认输入法时安全性最差,而自绘随机软键盘的安全性能最好。

1) 系统默认输入法

系统默认输入法是指用户设置的默认输入法。系统默认输入法并不一定是系统自带的输入法,也可能是第三方的输入法。对于 Android 操作系统来说,用户一般使用“文本编辑框”(Edit Text)输入内容,而这一过程调用的便是系统默认输入法。因为默认输入法的实现是独立于操作系统和客户端软件的,是一个独立的软件,所以当用户使用默认输入法输入信息时,输入的内容其实是由输入法进程交给客户端程序。因此,一旦默认输入法程序感染了恶意代码,或该输入法被具有记录键盘输入功能的恶意代码控制,则会导致所有输入的信息被窃取。

2) 自绘固定软键盘

出于安全考虑,像网上银行等对输入安全要求高的移动终端客户端会在密码输入框处使用自己绘制的密码输入键盘,以避免可能出现的被第三方输入法程序窃取这一风险。不过,当自绘软键盘采用固定分布方式时,由于每次打开输入法时出现的软键盘上字母、数字和特殊符号的分布位置是固定的,恶意程序可以通过记录用户在屏幕上的单击位置信息,再配合自绘固定软键盘的功能设置来猜测用户输入的信息。

3) 自绘随机软键盘

自绘随机软键盘是安全性最高的一种软键盘输入方式。由于每次打开软键盘时,字母、数字和特殊符号在键盘上的分布位置是随机性的,因此可以大大提高攻击者的门槛。因为,恶意程序即使记下了用户在屏幕上的单击位置信息,但能够正确猜测具体输入内容的可能性是很小的。

2. 软键盘输入的安全

对于网上银行等安全要求高的客户端,在使用输入法时建议采用自绘随机软键盘方式。在移动终端客户端输入过程中,很多人习惯于使用分布格局与传统键盘相同的软键盘输入方式(绝大多数自绘固定软键盘都是这样),对于字符分布没有规律的自绘随机软键盘方式不太喜欢,甚至认为很麻烦,产生应用上的抵触情绪。对于有这种认识的用户来说,必须强调这样一个事实:安全与便利之间是成反比的。

需要说明的是,在信息领域没有绝对的安全,输入法也是这样。虽然自绘随机软键盘大大提高了输入法的安全性和被攻击的难度,但如果攻击者针对某个(如某一网上银行)客户端软件事先植入了恶意代码,攻击者同样也能够窃取到用户输入的信息。对于这种极端攻击现象,一般是很难预防的。

7.2.3 盗版程序带来的安全问题

大量的免费下载网站为用户下载各类应用软件提供了便利。但是,部分网站对上传的应用软件审核不严,使许多带有恶意代码的软件被上传并通过网站传播,为用户安全带来了极大威胁。

1. 逆向工程

逆向工程也称为“反向工程”,在信息技术领域是指对一个信息系统或软件进行逆向分析及研究,从而得到系统或软件的架构和开发源代码等要素,进而对其进一步分析或优化处理。

攻击者也可以利用逆向工程原理和思路,采用逆向分析工具对一些自认为有利用价值的软件进行反编译,并在反编译后的程序中加入恶意代码,经再次编译(二次打包)后上传到一些审核不严的免费网站(如手机应用商店、手机软件商店等),供用户下载,以达到入侵和窃取用户信息的目的。

对于大量使用的基于 Android 开源系统的应用软件,目前出现了许多汇编和反汇编工具,如 Smali 和 Baksmali。首先,使用 Baksmali 工具对有利用价值的客户端软件以及木马程序进行反汇编,然后对反汇编结果进行整合(整合过程中还会尽可能地隐藏木马程序的代码),之后再利用 Smali 工具进行汇编编译,生成最后的二次打包可执行文件(DEX 文件)。

2. 二次打包

利用 Android 操作系统的漏洞,通过在反汇编后的程序中隐藏木马代码,以达到篡改原始客户端软件的执行流程、截获用户的账号信息和隐私信息等目的。经过二次打包后的应用软件,其界面和操作与原软件几乎没有区别,对于隐藏的威胁普通用户几乎无法感知。

经国内一些专业安全公司分析,目前几乎所有的银行客户端软件均未能完全有效防范逆向分析和二次打包,不具有防止逆向分析和二次打包的可靠能力,大量与用户贴身利益相关的移动客户端软件都存在盗版现象,而且某些软件还存在多个甚至是几十个不同的盗版版本。业内很有概括性的一句话描述为:正版下载量越大,盗版版本数也就越多。

例如,已发现的针对 Android 操作系统的“XX 神器”,就是攻击者将病毒二次打包后再上传到一些热门手机应用商店中供用户下载,利用手机论坛、非安全电子市场进行传播。该病毒可通过读取用户手机联系人,并调用发短信权限,将内容为“(手机联系人姓名)看这个 + **** /XXshenqi.apk”发送到手机通讯录的联系人手机中。当该手机通讯录中的用户接收该短信,不小心点击了链接并选择了“安装”后,在用户完全不知情的情况下,该病毒开始再向用户手机通讯录中的联系人群发同样的短信,从而导致被该病毒感染的手机用户数呈几何级增长,而且该病毒可能导致手机用户的手机联系人、身份证、姓名等隐私信息泄露,在手机用户中形成严重恐慌。

3. 防范方法

防范二次打包的有效方法主要有对 APP 进行签名验证,以及对 APP 进行加固处理等方式。

1) 签名验证

在应用程序发布时,每一款应用程序都会有一个专门针对该款软件的数字签名,用此验证软件的具体身份信息,不同厂商的软件其数字签名不同。由于数字签名是无法伪造的,因此利用该特征就可以知道一款应用程序是否为正版软件。对于加入了数字签名验证代码的软件,如果盗版者对其进行二次打包时没有去掉验证代码,则打包生成的盗版 APP 在运行过程中就会自动报警,被安全软件识别。但是,“道高一尺,魔高一丈”的道理在软件盗版领域显得尤为突出,如果盗版者具有较强的逆向分析水平,能够找到原 APP 的数字签名代码并移除或屏蔽,就可以避免报警。为此,要较好地解决此问题,单纯从软件技术上是无法实现的,目前最有效的办法仍然是采用验证技术,将安全性寄托在数字签名的证书管理上,通常可通过信誉度高的可信第三方(如知名 APP 安全软件商)负责对 APP 进行数字签名验证。

2) 加固处理

应用加固是近年来兴起的一种反盗版、防篡改技术,其基本方法是先将正版应用程序进行反汇编,之后对程序的汇编代码进行加密和混淆处理,然后再进行重新编译打包生成应用程序,同时由正版作者对经过加固处理的应用程序进行重新签名。经过加固处理的应用程序,虽然理论上仍然可以进行反汇编,但由于程序事先经过了加密处理,因此反汇编之后的代码的可读性将大大降低,相应地,盗版者对程序进行逆向分析的难度也大大增加,使得盗版者通常难以在原有代码中植入恶意代码,从而可以有效地阻止应用程序被二次打包和篡改。例如,国内安全厂商 360 从 2014 年 4 月开始推出的“360 加固保”(如图 7-6 所示, <http://dev.360.cn/protect/welcome/>)可以为手机 APP 开发者提供免费的加固服务,以防止产品被破解和篡改。



图 7-6 “360 加固保”页面

需要说明的是,自身带有数字签名验证能力的客户端软件通常不适合进行加固处理。这是因为加固处理本身就是一种对源码的重新组合,如果在加固之前没有移除源程序中的数字签名验证代码,那么数字签名验证代码就会将经过加固处理的应用程序视为盗版应用程序,并因此引起程序内部冲突。为此,在对移动终端上的 APP 进行加固处理之前,必须提前移除或屏蔽掉数字签名代码。

7.2.4 认证安全

认证即验证用户身份信息的合法性,例如,当用户登录自己的邮件系统或 QQ 账号时都要输入验证密码,这是对账户的真实性进行验证。许多安全场所都要求用户出示自己的身份证,对用户身份的真实性进行验证。为此,认证系统或认证方式决定着认证的安全性和认证效率。

1. 双因子认证

认证过程是用户(要求验证者)向认证服务器(验证者)输入自己的身份信息并验证其真实性的过程,是确保访问者合法性的重要环节。用户与认证服务器之间的认证可以基于如

下一个或几个因素。

(1) 用户所知道的东西,如口令、密码等。

(2) 用户拥有的东西,如印章、智能卡(如信用卡)。

(3) 用户所具有的生物特征,如指纹、声音、视网膜、签字、笔迹等。

如果认证过程中使用了以上其中一种因素(因子),称为单因子认证,如果同时采用了两种或两种以上的因素,则称为双因子认证或多因子认证。一次认证过程中,认证的安全性通常与参与认证的因素之间成正比关系。

基于传统单因子认证存在的安全风险,目前很多网络账号管理系统通常采用双因子认证甚至是多因子认证方式。在网络账户管理系统中,通常双因子认证中的一个认证信息是由用户自己掌握的,一般为账号对应的密码。而另一个认证信息是由双因子认证系统(认证服务器)提供的,如验证邮件、手机验证码、动态电子令牌或U盾等。为此,双因子认证的安全性也取决于两个认证信息之间的相互独立性。越是相互之间独立的信息,越不容易被攻击者在限制的短时间内同时截获。这里的独立性包括认证信息内容的相互独立,也包括认证信息传输途径或传输介质之间的相互独立。例如,当用户在计算机上进行网上银行支付时,虽然用户账户密码由用户直接输入,但验证信息却发送到该账户注册者的手机上,这就增加了攻击者获取验证码的难度。

但是,手机等移动互联网终端受自身众多因素的限制,如果要想实现与传统个人计算机上相似的双因子认证还存在一定的困难。例如,当用户利用手机进行网上银行在线支付时,一方面是通过手机来登录网上银行系统,并发送支付请求;另一方面又是通过手机来接收银行发回的短信验证码和确认信息。这在很大程度上限制了短信验证信息的独立性。将这种虽然使用了双因子认证方式,但却无法较好隔离不同认证信息的认证称为“伪双因子认证”。

目前,大部分银行客户端软件采用的是“账号密码+短信验证码”的伪双因子认证体系。这种认证体系在面对具有短信劫持功能的手机木马攻击时显得极为脆弱。

2. 验证短信的安全分析

对于使用伪双因子认证的移动互联网客户端软件来说,能否保证验证信息不被劫持和窃听,成为手机等移动终端认证安全性的决定因素。目前,包括网上银行在内的许多重要移动终端客户端软件还没有提供针对短信劫持的防范功能。如果终端被植入了短信劫持木马,那么银行等短信网关发送给用户的短信验证码、交易通知等各种重要信息就有可能被木马截获并自动转发给攻击者。

以银行网上支付系统为例,银行系统向用户手机发送验证短信以验证登录者身份的合法性,是基于“验证码只有手机拥有者本人可见”这一条件,如果手机被植入了木马,那么这一假设就不再成立。然而,在多数情况下,短信劫持木马为了避免被发现,往往会本地手机上采取短信拦截手段,即在转发银行短信给窃听者的同时,不会在手机上显示银行发来的短信。这样,攻击者就可以在用户毫无察觉的情况下,利用窃取的用户账户信息盗刷用户的手机银行账户。

目前,主流的短信劫持木马通常会劫持并自动转发手机验证码短信、密码找回验证短信、消费通知短信等多种短信信息,而且这些木马在转发信息的同时,还会在本地手机上销毁短信原文,以避免自身被暴露或被发现。

3. 防范方法

目前,解决像网上银行等重要应用中的伪双因子认证中存在的安全问题,主要采取以下3种防范方法。

1) 新技术的应用

通过对新技术的应用,将伪双因子认证改造成真正意义上的双因子认证。目前,市场上已经出现了一些专门针对手机银行等重要应用的双因子认证解决方案,如音频盾、蓝牙盾、电子密码器等。以工商银行提供的音频盾为例,它可以通过与手机上的音频口(耳机接口)相连(图 7-7),用于手机银行的数字签名和数字认证,对交易过程中的保密性、真实性、完整性和不可否认性提供安全保障。蓝牙盾的工作原理类似于音频盾,只不过是手机上的蓝牙接口进行连接。而电子密码器则与传统的动态电子令牌相似,它与手机银行客户端配合使用。

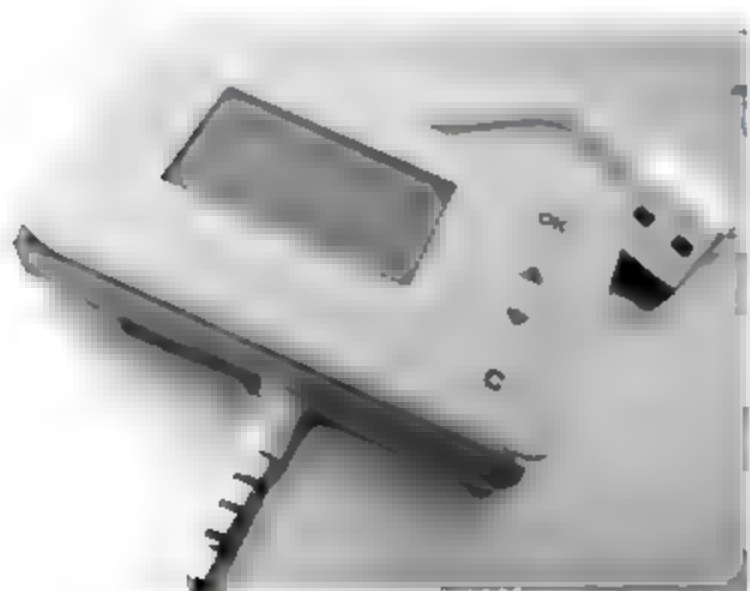


图 7-7 音频盾的外形

不过,联想到近年来移动互联网的快速发展过程,应用的便捷性和易用性是决定用户接受程度的关键因素,如果单纯为了安全,在手机上额外增加这些大小和能耗接近于手机本身的部件,很不适合在移动环境中的应用。所以,对于新技术的研究还有很大的发展空间。

2) 权限管理

如果能够采取技术措施,使客户端软件能够早于木马程序获得短信信息并将短信内容直接通知和展示给用户,就可以避免木马劫持信息事件的发生。目前,最常采用的是类似于 Windows 操作系统“兼容模式”的 APP Hook 技术。通过 APP Hook 技术,可以提升客户端接收短信软件(短信接收 APP)的权限,以保证短信在以广播形式分发给木马程序之前被拦截,终止短信的分发。不过,从目前的应用来看,这种方式也存在以下一些局限性。

(1) 该方案要求手机客户端程序必须获得手机的 root 权限,这已大大超出了一般手机软件的能力。

(2) 使用该技术方案后,有可能导致手机客户端与其他应用之间产生权限冲突。

(3) 木马程序也可以采用同样的手段来争夺手机短信的优先阅读权限。

针对以上问题,从 Android 4.4 版本开始就将短信接收(SMS_received)广播方式改为无序广播,同时对应用程序删除短信的权限进行了更严格的限制。这种安全机制的改进大大降低了木马程序优先获取信息阅读权限的能力,同时使木马程序失去了销毁短信的能力。但是,即使木马程序无法优先读取和销毁短信,但木马程序仍然有能力监听短信内容,所以针对 Android 等任何一款操作系统,其安全仍然是一个长期研究和逐步解决的问题。

3) 短信加密认证

在无法确保验证短信不会被恶意程序窃取的情况下,对短信内容进行加密这一看似传统的方法,却成为一种有效的解决方案。短信加密认证,就是由认证服务器厂商对发送到用户手机的短信进行加密,用户手机在接收到短信后,再通过手机客户端中的安全模块对接收到的加密短信进行解密操作,最后得到短信明文的过程。在这种安全机制中,由于手机收到的验证短信为密文,即使被木马程序截取也无法直接获取有效信息。更客观地讲,即便是恶

意程序对加密验证码进行了暴力破解,此过程所需要的时间通常也远远超过了该验证码的实际有效期,这样就可以从根本上解决 Android 系统短信验证码被泄露的问题。

7.2.5 安全事件分析

本节前面的内容主要以 Android 操作系统为例,介绍了移动终端系统本身的安全问题。这并不意味着只有 Android 系统才存在安全问题,使用其他类型操作系统的移动设备就不存在此类问题。其实不然,从目前的统计数据来看,几乎所有的智能移动终端操作系统都存在不同程度的安全问题和风险。

1. 苹果 iPhone 擅自采集个人隐私事件

中央电视台在 2014 年 7 月 11 日的《新闻直播间》节目中曝光了苹果 iPhone 未经用户许可擅自采集个人隐私的事件。央视调查揭秘指出,在苹果 iOS7.0 版本中,用户只要在苹果手机上使用软件、连接 Wi-Fi,用户使用软件的时间、地点等日常行迹信息就会被完全记录下来。对于此质疑,苹果公司也首次公开承认了收集用户信息的事实,这一行为引发了国内用户的强烈不满,也为广大消费者敲响了警钟。根据央视对苹果安全事件的调查显示,苹果手机在我国拥有上亿台,而大部分 iPhone 用户对其擅自采集个人信息一事并不知情。

2. 手机预装恶意软件

在 2014 年央视“3·15”晚会上,手机预装恶意程序被曝光。央视的调查显示,名为鼎开联合的公司可以经过手机植入平台,为合作商户的手机量身订做软件包,可以做到让用户想删都无法删掉。有些预装软件还能够监测用户的使用情况,仅仅这一项预装业务每年为公司能带来不菲的收入。另一家大唐高鸿技术有限公司,是大唐旗下的公司,大唐神器号称全自动智能安装软件,这款产品就是与手机商合作的。在事件曝光时,他们有 1404 家加盟代理商,安装软件超过 4600 万个。图 7-8 所示的便是在手机上预装的一些软件,其中一些便是恶意软件。

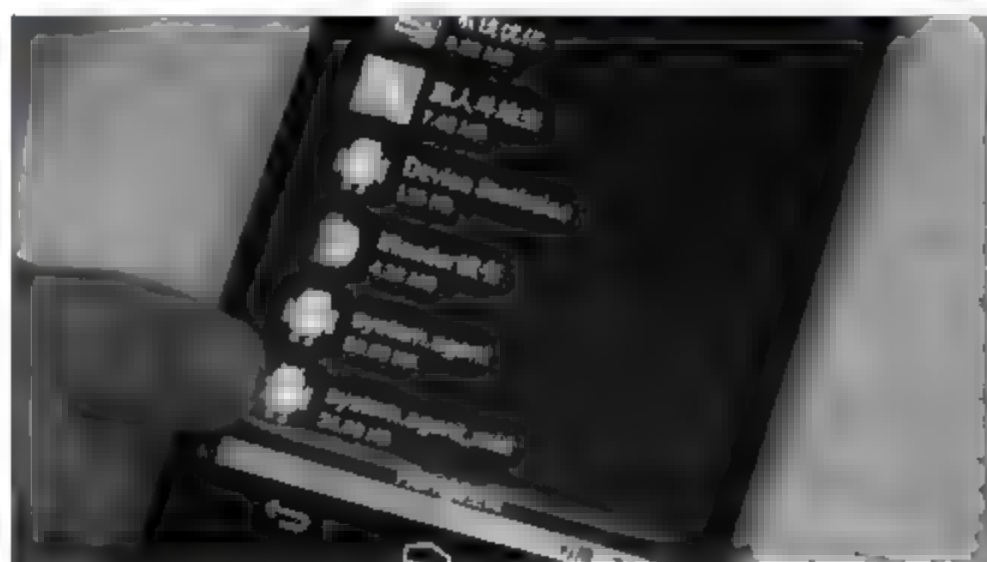


图 7-8 手机上预装的一些软件

现实世界中还有一种更为“暗黑”的应用推广方式“静默渠道”,这种应用推广渠道已有非法之嫌。具体方式为与手机厂家深度合作,将留有“后门”的软件内置在出厂手机中,通过“后门”远程控制这些应用,在后台偷偷下载安装其他程序。不需要用户确认就能直接安装,而且安全软件也无法查出来。

3. Android“诈尸”漏洞

2014 年 3 月 26 日,安卓手机系统被曝存在一个新的高危安全漏洞“Android 诈尸漏

洞”,利用该漏洞黑客可通过简单的攻击代码使被入侵手机崩溃后不断进行重新启动操作,只有通过恢复出厂设置才能修复,但手机中所有数据将因此彻底丢失。

当安卓应用(APP)的名称长度大于 387 000 个字符时,一旦运行就会造成手机关键系统进程崩溃,导致关机无法正常使用,如果该应用为开机自启动,这将导致手机开机后再次崩溃,最终导致手机进入循环死机的状态。安卓系统 2.3、4.2.2 和 4.3 等主流版本都发现存在该漏洞。

7.3 移动应用的攻防

本节以手机应用为主,介绍移动应用面临的主要安全问题和安全威胁,以及对应的安全措施和安全防御方法。

7.3.1 恶意程序

与个人计算机中对恶意程序的定义类似,移动终端中的恶意程序也通常是指带有攻击意图的一段程序,主要包括陷门、逻辑炸弹、特洛伊木马、蠕虫、病毒等。随着移动互联网的发展,针对新出现的恶意攻击现象,对手机等移动终端上的恶意程序类型进行了细分。

1. 恶意程序影响

最近,根据“中国反网络病毒联盟”分类标准,目前可将移动终端恶意程序分为资源消耗、隐私窃取、恶意扣费、诈骗欺诈、流氓行为、系统破坏、远程控制和恶意传播几种类型。其中,感染量最大的为资源消耗类恶意程序,其主要恶意行为是通过自动联网、上传和下载数据、安装其他应用,消耗用户手机流量和资费。

2. 恶意程序事件分析

1) “窃听大盗”木马

“窃听大盗”木马通过论坛链接、扫描二维码等方式骗取用户安装。安装之后手机会自动重启,重启后手机桌面并没有任何新增图标。“窃听大盗”木马会偷录用户的通话语音,调用摄像头偷拍手机周围环境,窃取通讯录、通话记录、短信文本等全部隐私信息,并能定位用户的地理位置,随后将这些信息发送到木马作者的邮箱。同时,由于安装前激活了设备管理器,导致用户根本无法正常卸载该木马。近期截获的“窃听大盗”木马二代则伪装成多达几百款软件欺骗手机用户下载,拨号器、Wi-Fi 万能钥匙、百度、91 助手、淘宝等几百款软件均被其“冒名顶替”。这些恶意程序通过开机自启动、定时器触发、短信触发 3 种方式执行窃听行为。更为隐蔽的是,一旦被触发,恶意程序会进入系统预装列表,手机用户无法正常卸载。

2) Android“长老”木马

2014 年 3 月 6 日,有一种潜伏在手机预装 ROM 中长达三年的“长老级”手机木马首次被发现,从 2011 年以来已衍生出十几个变种,最新变种不但会窃取用户手机号、IMEI (International Mobile Equipment Identity,移动设备国际标识码,是由 15 位数字组成的“电子串号”,它与每台手机一一对应,而且该码是全世界唯一的)及地理位置等隐私信息,同时还强制手机小组件来推广广告,还可以篡改手机浏览器主页、偷偷安装其他未知手机应用。

该“长老”木马甚至还可根据窃取的手机号码单独控制某一款手机,替换 Android 系统正常进程 Debuggerd 来实现自启动,用户不会在启动程序中看到它,行为非常隐蔽。木马运行后会立即释放多个 apk/jar/elf 等木马“小弟”恶意程序来实施破坏。“长老”木马有着极强的远程控制手段。不但支持网络和短信两种远控模式,并且带有十几个可配置参数,甚至可对某台手机单独控制,将手机彻底沦为“肉鸡”。为了更好地控制这些配置参数,木马还会启动一项服务专门用来监控系统时间,如果重启手机后 Wi-Fi 开启,将立即更新配置文件,如果没有 Wi-Fi 或者超过一天没有重启,会在 22 点到零时的整点,尝试通过上网流量的方式进行更新。更新的同时,还会将隐私信息上传至指定的服务器。

3) “夺命锁”木马

2014 年 6 月出现的“夺命锁”木马可以伪装成“天天酷跑专用修改(超哥破解)”“妖艳制作”等 600 余款手机应用,诱骗安卓手机用户进行下载,当手机用户不小心下载安装后手机会被强制锁死,24 小时无法正常使用,采用重启手机的方式仍然无法解决。

3. 安全防范方法

对于以上恶意程序存在的风险,建议从以下几个方面加强安全管理。

(1) 不随意点击不明链接。由于绝大多数木马程序是通过 QQ 或微信等方式来发送链接,在收到不明链接或网上购物时,一定要验证发送者信息的真实性。

(2) 平时养成关闭 Wi-Fi 或蓝牙功能的习惯,一方面防止黑客在公共场所通过 Wi-Fi 或蓝牙对手机进行攻击并窃取信息,另一方面可有效节约电能,并可以预防通过 Wi-Fi 实施定位。

(3) 及时备份手机等移动终端中的数据,尤其是一些敏感数据,以防止手机因攻击导致无法正常工作,需要初始化时不至于丢失数据。

(4) 从运营商、专业供应商或信誉度高的手机软件商店处更新软件固件,避免到一些不明身份的第三方站点下载和安装固件。

(5) 为手机设置流量提醒功能,避免手机不幸感染病毒或恶意软件后台偷偷联网造成资费消耗。

(6) 不要随意用手机扫二维码,二维码已经成为恶意程序新的传播途径。

(7) 从有安全信誉的来源下载应用程序。

7.3.2 骚扰和诈骗电话

到目前为止,中国已经实现了每人至少拥有一部手机。相应地,借助手机进行欺诈或扣费的多种骚扰和诈骗电话开始泛滥,轻则人们的生活造成影响,重则导致用户经济损失或名誉受损。

1. 骚扰电话

骚扰电话以短时间振铃为特征,用户通常情况下无法正常接听,其呼叫违背手机用户的意志并且对用户的通信自由、生活安宁造成侵害或者蒙蔽用户的呼叫。绝大多数响一声电话都是声讯台等吸费电话,有些声讯台还设在国外,一旦拨打回去,手机资费就会快速地被消耗殆尽;而广告推销类骚扰电话则是人们感受最深的骚扰电话,类似推销保险、推销贷款、推销商铺等业务之类的电话频频骚扰用户的日常生活。骚扰电话一般具有以下特征。

(1) 大批量呼叫。大批量呼叫是指针对批量手机目标号码发起呼叫或对单一目标号码的反复呼叫。针对单一用户的大批量呼叫违背了手机用户的主观意愿并且对用户造成了骚扰。

(2) 反向验证不正常。通过对主叫号码进行反向呼叫测试,如果播放欺骗信息或诱骗用户拨打声讯台等,都将视为骚扰电话号码。

(3) 违背用户主观意愿。这是骚扰电话的主要特点之一。骚扰电话号码对被叫用户而言都是陌生号码,或者是根本不存在的虚拟号码,通过该号码强制对用户进行呼叫。这些呼叫行为都是违背用户主观意愿的,对被叫用户而言是无效的呼叫。

(4) 对用户造成骚扰。这是骚扰电话的另一重要特点。骚扰电话均以短间接通为特征(如响一声),在用户正常接通前就已经挂断,以期用户进行反向拨打,从而达到其不法目的,这对用户的正常通信造成了骚扰。

2. 诈骗电话

诈骗电话(也称电信诈骗)是指借助手机、固定电话、网络等通信工具和现代网络技术实施的非接触式诈骗活动。开始时诈骗者通常会抓住一些人贪图小利、避险消灾等心理,不断变换手段实施诈骗,使受害人承受财产损失和精神骚扰的双重伤害,给人们造成了巨大的财产损失,社会危害不断加剧。诈骗电话一般具有以下特征。

(1) 诈骗手段多样。目前,主要的诈骗手段可分为以下几种类型。

① 假冒国家机关工作人员进行诈骗。

② 冒充电信等有关职能部门的工作人员,以电信欠费、送话费、送奖品为由进行诈骗。

③ 冒充被害人的亲属、朋友,编造生急病、发生车祸等意外急需用钱,或称被害人家人被绑架索要赎金等事由,骗取被害人财物。

④ 冒充银行工作人员,以假称被害人银联卡在某地刷卡消费为名,诱骗被害人转账实施诈骗等。

(2) 有组织的集团作案。该类事件组织化程度高,犯罪分子以诈骗为常业,有固定的诈骗窝点,作案时分工明确、组织严密,且大都使用假名,呈现明显的集团化、职业化特点。

(3) 迷惑性强。不法分子首先通过有关手段得到用户的电话(固定电话或手机号码),再利用改号软件使被害人的电话来电显示拨打过来的电话是110、12315或电信10000等常见的业务电话,或是被害人熟悉的亲友的电话,使被害人相信对方确实是公安、工商或电信公司的工作人员,或是自己的亲友,从而放松警惕。

(4) 实施手段隐蔽。不法分子往往只通过电话或短信的方式与被害人进行联系,从不直接和被害人见面,电信诈骗的组织者几乎从来不抛头露面。

(5) 社会危害大。该类事件的诈骗范围广,诈骗数额大,动辄就是几十万上百万元,使受害人蒙受巨大财产损失,严重扰乱社会经济秩序。相对于普通诈骗中“一对一”或者“一对多”的诈骗,电信诈骗表现出来的是面对整个电话用户或者特定群体的诈骗,其诈骗行为的实施并不是特意针对特定对象,而是广泛散布诈骗信息,等待受害者上钩。这种方式带来的后果往往是大批的电话用户上当受骗,涉案数额往往很大,对社会的危害极其严重。

3. 安全防范方法

电信诈骗的实质是利用社会工程学手段,抓住人性的弱点,通过手机、固定电话和计算

机网络等方式,对用户实施的一种犯罪行为。可以从以下几个方面防范电信诈骗。

(1) 不贪婪。不要轻信中奖的电话和短信,要明白“天下没有免费的午餐”这一基本道理,当接到不明身份的人员发过来的所谓中奖短信时,直接将其删除即可,切莫急于兑奖或按对方的指示支付给对方款项(如预交个人所得税、预交手续费等)。

(2) 不轻信。不要相信任何“紧急通知”。当在ATM自动取款机取款过程中出现操作故障时,不要相信贴在ATM机旁纸条上的任何“紧急通知”上的所谓“银行值班电话”,而应拨打银行正规的客服专线请求帮助。

(3) 多防范。对于来历不明的电话要谨慎小心,防止不法分子借机诈骗,如接到“猜猜我是谁”这种电话时,不要急于说出对方的名字,也不要透露自己更多的信息。如有人以电信工作人员或冒充民警打电话调查欠费并索要个人信息的,千万不要急于转账或透露个人信息,要通过正规渠道核实电话是否欠费,核实对方的身份,或者及时拨打“110”进行报警、咨询。

(4) 添加到黑名单。现在几乎所有的智能手机都提供了黑名单功能,或通过下载手机防火墙安全软件来实现黑名单操作。目前,有一些专业的手机安全软件本身就提供了对骚扰电话的自动屏蔽功能。对于已确定的骚扰电话,可以直接添加到黑名单中,如图7-9所示。

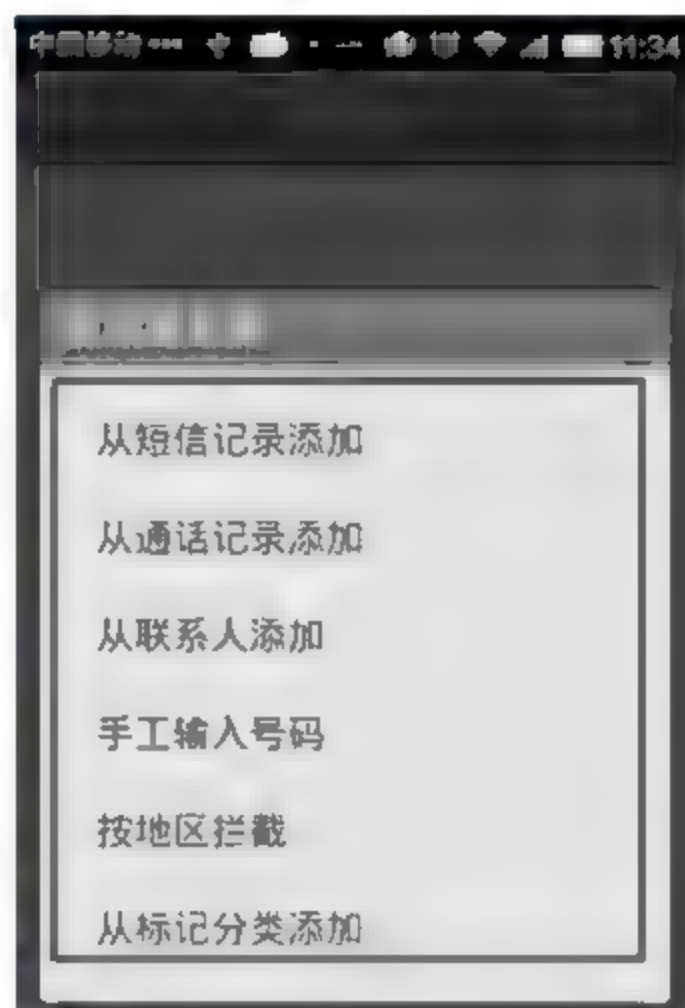


图 7-9 手机黑名单操作

7.3.3 垃圾短信

当移动手机几乎成为人手一机的通信工具时,随着手机输入法的不断丰富和便捷,手机短信已成为人与人之间一种极为便捷的交流方法。与此同时,利用手机短信进行诈骗的现象开始泛滥,不仅严重侵犯了人们的财产安全,而且破坏了正常的社会经济秩序。

1. 垃圾短信的概念

垃圾短信是指未经用户同意向用户发送的与用户意愿相违背的短信息,或与国家法律法规相违背的短信息,或用户不能根据自己的意愿拒绝接收的短信息。垃圾信息主要包括广告推销、诈骗信息、违法信息(如代开发票、赌博、博彩、办证、电话卡复制、色情服务、枪支出售等)。相比于在媒体上进行广告投放,群发垃圾短信的推广成本要低得多,而且事后追查相对较难,已严重影响到人们的正常生活及移动运营商的形象,甚至是社会稳定。

诈骗短信是垃圾信息中一种特殊的形式,是指以非法占有为目的,向手机用户发送虚假或隐瞒真相的短信,骗取公私财物的行为。手机短信诈骗是传统诈骗与现代通信技术相结合而产生的一种新型诈骗行为。诈骗短信要求接收到短信的用户进行转账或汇款;或冒充银行工作人员诱导用户点击恶意网站地址链接,访问伪造的银行钓鱼网站;或冒充律师、法官、警察等工作人员,可以帮助用户从监狱或看守所等地方“捞人”,提前释放等。

例如,有些不法分子在获得了部分具有特殊背景的人员信息后,就可以发送类似于“你的朋友××正在××看守所,我可以找人疏通关系放出,事后结算,联系手机 1330401××××”。这类诈骗短信正是利用了人们侥幸心理实施诈骗,他们在骗取钱财后往往会失踪。

其实,只要静下心来略作思考就会知道这是不可能的,因为所谓“捞人”本身就是违法的,不仅捞不出人,反而有可能会使人财两空。

再如,当你收到类似“恭喜您的手机已被《中国最强音》选为场外幸运号,您已获得苹果手机及5万元现金,请你登录网站 <http://www.zxx66.com>,验证码9800”的冒充热门电视节目中奖类短信时,如果你从未参加过相关电视节目的抽奖活动,就不要轻信任何此类短信。如果你确实参加了此类节目,可到官方网站查询或通过官方联系方式确认。

2. 银行“电子密码器升级”诈骗短信

电子密码器是银行面向电子银行客户推出的新一代安全认证工具,为网上银行、电话银行、手机银行等电子银行用户提供更加安全、可靠的身份认证服务。它是继U盾、口令卡之后的新型安全工具,通常内置电源和密码生成芯片,外带显示屏和数字输入键盘。图7-10所示的是一款工商银行的电子密码器产品。



图 7-10 工商银行电子密码器外形示意图

由于电子密码器具有开机密码保护、无须安装驱动程序、便于携带、为每个交易产生专属的密码、无须连接计算机等设备等特点,除可以用于普通的网上银行、手机银行、电话银行外,还可用于iPhone/Android手机银行、iPad网上银行和Mac计算机网上银行这些无法使用U盾进行安全认证的应用环境,极大地方便了用户,得到了广泛应用。不过,当安全技术在不断发展的同时,不法分子的诈骗手段也在不断翻新,他们可以通过一些技术手段模拟人们熟悉的可信银行官方号码发送钓鱼欺诈短信。例如,十堰市茅箭区陈女士接到一条由号码106071995588发来的短信,内容是“尊敬的用户:你的电子密码器将于次日失效,请尽快登录 www.icbco.com 进行安全升级,给您带来的不便敬请谅解!”落款是“工商银行”(如图7-11所示的是类似的短信)。之后,陈女士的女儿根据短信中的网址登录后,按照页面提示,先后输入银行卡号、密码、身份证号等信息,按照提示逐项完成操作后,网站显示密码修改升级成功。稍后,陈女士收到工商银行短信提示,称其工行卡上322088元存款全部被转走。

3. 安全防范方法

对于垃圾和一般诈骗短信,当用户对短信中透露的相关信息有疑问时,一定要通过正规



图 7-11 利用电子密码器升级的诈骗短信

渠道核实账户信息,不要独自做出判断并急于按短信提示进行操作(如银行转账、访问钓鱼网站等),也不要轻易将卡号、存款密码、个人身份等重要信息告知他人。通常情况下,银行、公安、司法部门都不会通过电话询问用户的存款密码,以及要求转账。

对于利用银行“电子密码器升级”这类新型的电信诈骗,由于人们对银行官方号码一般都比较熟悉,很容易轻信由银行号码发来的短信,并按照信息中的提示登录钓鱼网站,结果造成银行卡号和密码泄露,产生的后果非常严重。从对破获的此类案件来看,用户手机能够接收到类似于“95588”等银行发来的诈骗电话,主要有以下两种手段。

(1) 不法分子伪装成“95588”等银行官方号码,通过“伪基站”向周边用户手机发送短信。

(2) 手机系统存在短信欺诈漏洞,恶意 APP 也可以伪造任意号码向手机用户发送诈骗短信。

图 7 12 所示的是由 360 互联网安全中心提供的利用“官方号码”短信钓鱼诈骗的过程示意图。

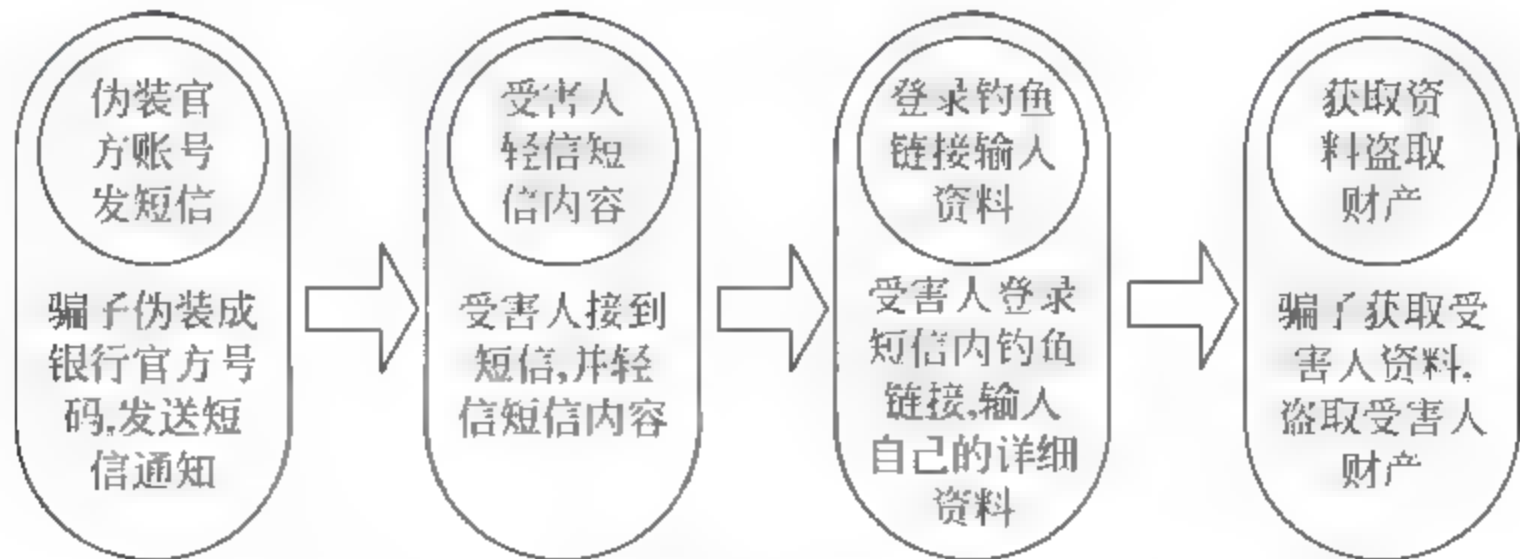


图 7-12 短信钓鱼诈骗的过程示意图

对于利用银行“电子密码器升级”的诈骗短信,用户应直接与银行工作人员联系,或到银行网点柜台办理,绝对不能通过短信中的网址登录网银。也就是说,提高警惕是防范此类诈骗的有效方法。

7.3.4 二维码安全

扫描二维码已经成为手机一族最流行的查询和互动方式。网上购物、添加好友、物品真伪鉴别,通过手机扫一扫就可以轻松完成。不过,二维码木马钓鱼诈骗等方式已开始出现,并不断更新欺诈手段,骗取用户钱财。

1. 二维码简介

二维码是用特定的几何图形按一定规律在平面(二维方向)上生成的黑白相间的具有唯一性的图形。由于图形的唯一性,因此二维码具有了在互联网上进行信息验证的功能。在移动互联网中,二维码的应用非常广泛,如产品防伪/溯源、广告推送、网站链接、数据下载、商品交易、定位/导航、电子凭证、车辆管理、信息传递、名片交流、Wi-Fi共享、手机支付等。随着智能手机的普及,手机“扫一扫”功能的应用,使二维码的使用更加普遍。

手机二维码是指以手机等移动终端和移动互联网作为二维码的存储、解读、处理和传播渠道而产生的各种移动应用服务。根据手机承担存储二维码信息或解读二维码信息的功能不同,通常又可将手机二维码服务分为手机被读类应用以及手机主读类应用两大类。

1) 手机被读类应用

手机被读类应用通常是以手机存储二维码作为电子交易或支付的凭证。终端用户通过各种在线或非在线方式完成交易后,二维码电子凭证通过移动网络传输并显示在手机屏幕上,可通过专用设备识读并验证交易的真实性。这类应用的特征主要有以下几点。

- (1) 手机以实现二维码的接收和存储功能为主,不对其承载的业务信息进行解析。
- (2) 需要专用设备对手机二维码图像进行识读。
- (3) 识读后的业务处理通常由专用设备执行,而与手机不直接相关。

这类业务中,二维码在被识读后通常还需要与后台交易系统交互,对其真实性和有效性进行检验。典型应用包括电子票、电子优惠券、电子提货券、电子会员卡和支付凭证等。

2) 手机主读类应用

手机主读类应用是将带有摄像头的手机作为识读二维码的工具,手机安装二维码识读客户端软件,客户端通过摄像头识读各种媒体上的二维码图像并进行本地解析,执行业务处理,还可能与应用服务器发生在线交互,进而实现各种复杂的功能。这类应用的特征主要有以下几点。

- (1) 二维码图像一般印刷在纸媒、户外等平面媒体上。
- (2) 依赖于手机客户端软件进行识读。
- (3) 手机客户端软件执行全部或部分业务处理。

典型应用如名片、短信、上网等,根据业务内容的获取方式还可分为“在线模式”与“离线模式”。名片应用是手机客户端将从二维码图像中识读的信息存入手机本地的通讯录;短信应用是客户端从二维码图像中读取内容和特定号码,调用手机短信功能将内容发送给该号码;上网应用是客户端从二维码图像中读取网站地址,并自动发起到该地址的链接,获取信息、广告或其他服务。目前,互联网中的二维码应用主要是手机主读类应用。

2. 事件分析

这里通过两个针对淘宝网购的二维码木马钓鱼欺诈事件,在回顾事件过程的基础上,分析利用二维码进行网络诈骗的特点。

(1) 2013年河南淘宝店主王某接收到一买家发来的二维码,该买家称因其需求量较大,怕买错款式,所以特地制作了一个二维码清单,要求王某只需要用手机扫描该二维码就可以知道自己要购买的所有商品。结果王某未经思考就直接扫描了该二维码(图7-13),随后出现了一个名为“购物清单”的APK文件下载页面,王某也按照系统提示进行了下载安装,但结果只有几行乱码,根本没有看到任何商品信息。但没过几分钟,王某的计算机上弹出了他的支付宝在异地登录的提示信息。当他感觉有些不妥并要立即修改支付宝密码时,却发现密码已经被人修改。



图7-13 用手机扫描接收到的二维码

在该事件中,黑客向王某发送了隐藏有木马钓鱼网站的二维码,当王某下载了该木马并自动启动后,王某手机接收到的所有短信都会被木马拦截并与王某的手机号码一起发给黑客。然后,黑客会利用其手机号码作为支付宝用户名,进行短信重置密码的操作,从而成功盗刷王某的网银。期间,因为手机短信被拦截,所以黑客的所有操作王某完全没有察觉。

(2) 2014年的一天,受害人谢某在淘宝商城购买了一件衣服并成功付款后,却收到了一个由卖家发来的二维码,并告诉谢某:扫描二维码后,可获赠免费的运费险,如果运输途中货物丢失或损坏,可以直接由保险公司来赔偿。对于免费的保险,谢某很自然地用手机扫描了二维码,并按照提示登录了“淘宝网站”(其实是假冒淘宝的钓鱼网站),并按提示输入了淘宝密码、支付密码及手机验证码等信息。但在提交后,系统出现“运险费授权失败”的提示,并且重复了多次输入后仍然如此。当谢某产生怀疑时,却发现原来的订货记录突然变成了“确认收货”,并且钱已经打到了对方账户。

与上一欺诈方式不同的是,本事件中的诈骗对象由原来的淘宝卖家变为买家,以赠送“运险费”为诱饵诱骗买家上当,进而盗取其支付宝账号和密码,并实施盗刷。

二维码支付主要应用于移动支付领域,并广泛应用于出租车、商场、超市等支付方式中。例如,“快的”“滴滴”打车软件,以及一些商场和超市推出的扫码支付,只要对准二维码“扫一扫”,就可以直接通过支付账户付款,非常方便。但从现状来看,一方面是二维码应用的快速发展,另一方面是二维码技术在移动支付中还没有相关的技术标准和检测认证标准,存在一定的应用风险。

3. 安全防范方法

作为一项新应用,二维码因其使用便捷、技术要求不高,从其问世便得到了广泛应用,同时二维码技术也成为手机病毒、钓鱼网站传播的新渠道。除针对淘宝网店的欺诈外,送保险、送礼品、打折等借口通常也是二维码钓鱼过程中常用的诱饵,当用户一旦贪小便宜进而扫描了二维码后,就会被诱导到钓鱼网站,盗取用户的个人信息,骗取钱财。还有部分链接是由不法分子伪装的吸费木马,一旦下载就会导致手机自动发送信息并扣取大量话费。

二维码本身不会携带恶意代码,但很多木马软件可以利用二维码下载。然而,很多手机

目前都使用开放式的手机平台,如果下载了这样的木马程序,木马程序就会“接管”手机的短信发送接口,在用户不知道的情况下发送短信。这类短信往往都要扣除高额的话费。

为尽量减少利用二维码隐藏的木马程序带来的危害,用户在扫描二维码前应先判断发布来源是否权威可信。一般来说,正规的报纸、杂志,以及知名商场的海报上提供的二维码是安全的,但在网站上发布的或由 QQ 发送的不知来源的二维码需要引起警惕。如果通过二维码来安装软件,安装好以后,最好先用杀毒软件扫描一遍再打开。当部分用户习惯于使用二维码时,可以选用有识别功能的扫码软件进行实时监控,如 360 安全卫士等。

除二维码隐藏的恶意代码外,二维码安全问题还存在于二维码扫描软件中,有些二维码软件提前内置了恶意代码,一旦安装就会遭遇恶意广告和扣费等问题。为此,在选择二维码扫描软件时也一定要到官方网站或一些知名网站下载。

7.4 云服务的攻防

云计算(cloud computing)是一种基于互联网的计算方式,通过这种方式,共享的软硬件资源和信息可以按需提供给计算机和其他凡是能够接入互联网的设备。云是对互联网的一种形象的比喻,云计算是针对传统计算而言的,它将传统的计算方式从本地计算机延伸到了互联网上(即“云端”),通过网络提供可伸缩的廉价的分布式计算能力。

7.4.1 关于云计算

2006 年,Google 提出“云计算”的概念。但在之前的 2002 年,Amazon 就已经推出了云计算产品 AWS(Amazon Web Service)。云计算虽然是一个新名词,却不是一个新应用。自有网络以来,人们就可以将文件上传到服务器的存储空间中保存,需要时再从服务器存储空间中下载文件。这种操作方式与今天人们使用的百度网盘、360 云盘、金山快盘、腾讯微云等模式没有本质上的区别,今天的应用方式只是提供了更加友好的操作界面并便于操作而已。

搜索引擎就是一种最简单且在网络服务中已经随处可见的应用工具,当人们在浏览器的搜索引擎中输入关键词时,搜索引擎便会在整个网络中进行搜索,并给出结果。今天的云计算,不仅仅只进行资料搜寻操作,还可以为用户提供各种计算技术、数据分析等服务。因此,就像搜索引擎一样,云计算也是一种服务,而且是一种更广泛的服务。如图 7-14 所示,利用云计算,人们用接入互联网的个人计算机、手机、PAD、电视机等终端,就可以在数秒之内处理数以千万计甚至亿计的信息,得到和“超级计算机”同样强大效能的网络服务,获得更多、更复杂的数据计算的帮助。

云计算是指 IT(Information Technology,信息技术)基础设施的交付和使用模式,指通过网络以按需、易扩展的方式获得所需的资源(硬件、平台、软件)。提供资源的网络被称为“云”,“云”中的资源在使用者看来是可以无限扩展的,并且可以随时获取、按需使用、随时扩展、按使用付费。这种特性经常被称为像使用水电一样来使用 IT 基础设施。

简单来说,云计算机可以将用户所需的软硬件、资料都放到网络上,在任何时间、任何地点,可使用各类接入互联网的 IT 设备(个人计算机、手机、平板电脑等),实现数据上传、下



图 7-14 云计算操作示意图

载、运算等目的。当前,常见的云服务有公有云(public cloud)与私有云(private cloud)两种。其中,公有云是基于互联网(Internet)的服务类型,广大互联网用户都可共享一个服务提供商的系统资源,他们不需要架设任何设备及配备管理人员,便可享受专业的IT服务。公有云还可细分为3个类别,分别是SaaS(Software-as-a-Service,软件即服务)、PaaS(Platform as a Service,平台即服务)和IaaS(Infrastructure as a Service,基础设施即服务)。例如,人们平时使用的Gmail、Hotmail、网上相册都属于SaaS的一种。而私有云则是由单位根据信息化应用需要在内部网络(Intranet)中建立的云服务系统,它的应用功能与公有云相同,只是应用范围受限而已。

对于普通互联网用户来说,云盘(云存储)是云计算中最为普及和大众化的一种服务方式。当云计算系统运算和处理的核心是大量数据的存储和管理时,云计算系统中就需要配置大量的存储设备,这时的云计算系统就转变成为一个云存储系统,所以云存储是一个以数据存储和管理为核心的云计算系统。云存储的普及,真正向普通用户证明了云计算时代的到来。

在移动互联网时代,个人计算机、手机、平板电脑、数字电视等成为人们经常使用的上网设备。如何实现同一信息源在不同终端上方便快捷地转存和浏览,就成为一个很现实的应用课题。云服务和云存储是目前解决跨平台信息交换问题比较有效的解决方案之一。同时,手机、平板电脑等移动设备的更新很快,而在更新后这些设备中存储的各种数据资料的备份也是一个不得不面对的问题,而云服务平台正好可以很好地解决这个问题。

此外,照片、视频等大文件的分享也需要云存储与云分享服务的支持。使用传统的邮件附件或FTP方式很难传送几十兆字节以上的文件,而且即使能够上传,分享起来也很不方便。而用云存储技术来分享一个大文件,用户只需向对方提供一个下载链接,对方就可以随时随地进行下载。分享链接不仅可以通过电子邮件进行传送,通过微博、网站等方式进行分享也非常方便,甚至已经有很多人开始使用云盘技术来搭建新型的文件下载服务器。

7.4.2 云存储的安全问题

相比于传统硬盘、U 盘和光盘存储方式,云存储具有存储量大(以 GB 为单位)、存储成本低(基本上都是免费)、数据不易损坏、不易丢失(由云存储服务商负责文件的安全备份)等安全性特点。不过,由于云存储作为一种基于互联网的应用,不仅要解决互联网已有的安全问题,同时也要面对这一新型应用特有的挑战与安全性威胁。

1. 云盘成为恶意程序传播的新途径

根据 360 互联网安全中心的监控,2013 年年初,已经出现了大量利用云存储传播恶意程序的事件。目前,平均每天截获的仅利用“360 云盘”进行传播的恶意程序文件和疑似恶意程序文件多达几万个。相比于各种传统的病毒传播机制,利用云存储空间传播病毒,成本更低,发现更难,而且具有较强的欺骗性。

2. 敏感信息存在安全风险

无论是企业还是个人,都有可能在云存储空间中存放一些私密或机密的文件信息,如涉及个人隐私或单位机密的照片、视频文件等。这些信息通常会面临两类主要的安全威胁:一是云存储空间账号被盗;二是云存储服务器中的信息被非法访问。而对于绝大多数用户来说,云存储服务器本身的安全性更受关注。用户只知道将数据放到了“云”端,但至于存在哪里,怎么存的,用户均一概不知。这种“神秘性”自然而然地失去了对安全性的认可度。

针对文件存储的机密性,许多云盘提供商采取了一些安全技术,主要有严格的权限和密钥管理,通过数据加密方式保证服务器中的数据安全,通过将同一用户的资料随机分散地存储在服务器的不同位置从而增加入侵者获取完整连续数据的难度等。如图 7-15 所示,360 云盘在分享文件时,对于机密文件设置了访问密码,以防范机密信息的不必要扩散。



图 7-15 为机密信息设置访问密码

3. 服务器损坏风险

云存储服务器也有可能受到如地震、水灾、电力中断等不可抗力的影响而发生数据损失。为抵御此类事故风险,一些云服务提供商通过采取将多个数据中心分布在多个机房,同时数据中心内多份复制并配备专门的备份数据中心的方式,保证数据在存储到数据中心后不会因事故的发生而丢失。很显然,服务器被损坏的风险越小,云服务提供商在数据备份方面的投入也就越大。

7.4.3 云服务的安全防范

目前,关于云计算与安全之间的关系一直存在两种对立的说法:持有乐观看法的人认为,采用云计算会增强安全性。通过部署集中的云计算中心,可以组织安全专家以及专业化安全服务队伍实现整个系统的安全管理,避免了现在由个人维护安全,由于不专业导致安全漏洞频出而被黑客利用的情况。然而,更接近现实的一种观点是,集中管理的云计算中心将成为黑客攻击的重点目标。由于系统相对庞大的规模以及前所未有的开放性与复杂性,其安全性面临着比以往更为严峻的考验。对于普通用户来说,其安全风险不是减少而是增大了。

从应用来看,云计算中用户将数据存储存储在云端,因而不拥有对自己数据的完全控制能力,只能依赖云服务商提供的安全保障,使用户能够信任新环境下的数据安全及完整性。相比于传统计算模式,这种数据新的访问和控制模式带来了新的安全挑战。为此,用户一般应选择规模大、信誉度高、安全措施得当的云服务提供商,以减小安全风险。另外,对于重要数据,当确实要通过云盘存储时,建议将同一份文件分别存放在不同的云盘上,实现用户端的安全备份。

云服务中的另一个问题是隐私保护问题。云服务要求大量用户参与,不可避免地出现了隐私问题。很多用户担心自己的隐私会被云服务提供者收集。正因如此,虽然在加入云计算时很多厂商都承诺尽量避免收集用户隐私,即使收集到也不会泄露或使用,但不少用户还是怀疑厂商的承诺,他们的怀疑也不是没有道理的。不少知名厂商都被指责有可能泄露用户隐私,并且泄露事件也确实时有发生。对于隐私保护问题,可从以下几个方面尽量避免。

(1) 行业自律。云服务提供商应规范行业行为,实现自我约束,协调同行利益关系,维护行业间的公平竞争和正当利益,促进行业发展,最大限度地保护云用户的个人隐私。

(2) 加强行业规范。一方面行业内对国家法律、法规政策的遵守和贯彻,另一方面是通过行业内的行规行约制约自己的行为。为了加大对互联网和云服务的安全管理,国家发展改革委等7部委联合发布了《关于下一代互联网“十二五”发展建设的意见》,其中强调:互联网是与国民经济和社会发展高度相关的重大信息基础。加强网络与信息安全保障工作,全面提升下一代互联网安全性和可信性。加强域名服务器、数字证书服务器、关键应用服务器等网络核心基础设施的部署及管理;加强网络地址及域名系统的规划和管理;推进安全等级保护、个人信息保护、风险评估、灾难备份及恢复等工作,在网络规划、建设、运营、管理、维护、废弃等环节切实落实各项安全要求;加快发展信息安全产业,培育龙头骨干企业,加大人才培养和引进力度,提高信息安全技术保障和支撑能力。

(3) 提高个人的安全意识。云服务在提供了快捷使用的同时,由于用户无法对云端资

源实现可控和可管,当出现一些安全风险时,将束手无策。受利益的驱使,不能确保所有的云服务提供商都是可信、自律的。另外,云服务中的用户数据等敏感信息,也已成为黑客地下产业链的重要信息来源。为此,对于用户来说,最有效的办法是将凡是涉及个人或单位信息的敏感数据,不存放在云盘中,即使部分云盘在数据存储时提供了数据安全加密功能,但任何安全技术和措施都是相对的。

(4) 加强技术管理。云计算作为一项新型应用技术,其安全性不仅涉及传统互联网中已有的安全问题,而且还必须面对新的安全威胁。例如,云计算环境中数据的传输、用户数据加密等问题都是传统互联网中涉及的,但云计算架构下的按需资源分配、跨域授权、隐私保护等问题,必须针对云计算理论体系和应用特点,做到有的放矢,提出有效可行的安全管理技术规范并加以实施。

7.5 网络购物的攻防

网络欺诈是指通过使用网络进行的各种欺诈行为,其目标的是通过现代信息网络并以欺骗手段非法获取用户名、密码、银行卡号、信用卡号、身份证号码、手机号码、邮箱地址、家庭地址等信息,进而用于非法活动。网络欺诈行为的发生数量每年都在增长,产生的社会危害很大,尤其是随着移动互联网的广泛应用,网络欺诈方式不断翻新,影响范围不断扩大,受害人数不断增长。与此相反的是,实施网络欺诈的条件却越来越简单,成本越来越低廉。

木马病毒和钓鱼网站是目前网络欺诈的常用工具和方法,由网络欺诈而导致的经济损失每年达到几十亿元人民币。作为一种“低投入、高产出”的网络犯罪行为,网络欺诈给普通网络用户造成的经济损失非常巨大。国内专业网络安全机构的统计结果显示,目前主要的网络欺诈形式和方法主要有网络兼职、虚假购物、网络游戏、账号被盗、虚假团购、话费充值、消费欺诈、网上博彩、虚假票务、网购木马、投资理财、视频交友和虚假中奖等。网络欺诈的传播方式主要有搜索引擎、即时通信(如QQ、旺旺等)、游戏平台、短信等,特别是不法分子通过QQ发送钓鱼网站或欺诈链接,以诱骗受害者上当。本节通过对几个典型案例的分析,介绍网络购物(简称“网购”)中存在的安全风险及应对方法,以期为大家起到警示作用。

7.5.1 网络游戏网站钓鱼欺诈

无论是传统互联网还是移动互联网时代,网络游戏都是最吸引用户和最为广泛的应用之一,网络游戏产业的发展呈现出蓬勃态势。同时,针对网络游戏网站的钓鱼欺诈现象也频繁发生,对游戏玩家造成了很大危害。

1. 案例分析

游戏玩家李某在玩某一网络游戏时,看到游戏公共频道有人在不停地发送“××搜索××游戏装备大赠送”的信息。于是,李某便到信息中提及的“××搜索”引擎中搜索“××游戏装备大赠送”这一关键词,果然该搜索内容显示在该搜索引擎的首条。当李某不假思索地点击搜索引擎提供的链接后,在出现的页面中要求李某输入游戏账号和密码。李某按提示输入后,结果系统却没有反应。一开始,李某以为网站出了故障,没有太在意。但几个小时后,当李某再次登录游戏后,却发现自己账户中的“装备”和“金钱”已经一无所有。

在本事件中,不法分子不是通过 QQ 或邮件方式将以“中奖”或“大赠送”为名义的钓鱼网站地址发给用户,而是告诉用户到搜索引擎中去查找该中奖信息的链接地址,使用户放松了警惕。此类事件由于不法分子在实施欺诈前已经掌握了部分用户的心理,以被大家普遍认为可信的搜索引擎作为行骗的中介,迷惑性较强。

近年来,网络游戏已经成为一个强大的产业,在互联网应用中占据着重要的地位,因此也成为不法分子进行钓鱼欺诈的重点。不法分子通过在各大知名游戏网站发送欺诈信息,出售一些明显低于市场价格的“装备”“游戏币”或冒充游戏官方发送礼品等行为,不断诈骗用户。在此基础上,再利用一些搜索引擎存在的漏洞,提升欺诈信息的排名,使部分游戏玩家上当。

2. 主要防范方法

网络游戏网站钓鱼欺诈的实现通常由 3 个环节组成:制作钓鱼网站、提升在特定搜索引擎中的排名和在游戏平台发送诈骗信息。其中,最为关键的一个环节是通过 SEO(Search Engine Optimization,搜索引擎优化)或参与竞价,把钓鱼网站排到指定搜索引擎的首条,以增加搜索结果的可信度和被点击的可能性。为此,防止此类诈骗的主要方法是用户可分别到多个搜索引擎中去查找,如果被查询信息仅仅在指定的搜索引擎中排在首位,而在其他搜索引擎中却查不到或排名靠后,则可以怀疑为虚假信息。

7.5.2 网络退款骗局

退款骗局是网购中出现较早的欺诈方法,随着网购规模的迅猛扩大,各类以退款为手段的欺诈层出不穷,并不断变换方式,以更大限度地迷惑和欺骗用户,对用户造成很大的经济损失。

1. 案例分析

2018 年 5 月,某地的吉先生在国内某知名网店购买了一件电子产品,当完成付款后不久便收到了一个自称是该网店客服的电话,称因为该网店系统临时维护升级,吉先生的订单失效,需要他填写退款协议办理退款。

不明真相的吉先生并不知道该网店退款办理中并没有这一流程,于是打开了对方通过 QQ 发来的退款链接。根据页面提示,吉先生依次输入了自己的银行卡号、密码、身份证号码、预留手机号码及短信验证码等信息。在单击“提交”按钮后,吉先生便收到了一条告知他的银行卡被消费了 3000 元的短信。

在该案例中,不法分子通过非法渠道获取了网购的客户信息,利用客户付款后等待收货这一时间段假冒网店卖家或客服,通过电话联系方式,以支付系统出现问题或升级等为由,诱导受骗者进行退款操作。随后,不法分子会给受骗者发送退款网站地址链接,受骗者通过链接打开高仿真钓鱼网站。钓鱼网站会诱导受骗者输入支付宝账号、密码、银行卡号、身份证号码、手机验证码等个人信息,盗刷用户支付宝和银行卡。

2. 主要防范方法

以上诈骗得以实施有两个非常重要的条件(或表象):一是吉先生的网购信息如此之快地被不法分子获得,进而不法分子冒充为网店客服实施诈骗,说明因个人信息泄露而导致的危害已非常严重,而且泄露速度之快令人震惊;二是由于受骗者打开的钓鱼网站的仿真度

极高,普通用户仅凭简单的视觉判断已很难辨别真伪,而制作高仿真度的网站在技术上早已没有门槛。

对于该类骗局,可通过以下方法防范。

(1) 在网购过程中,凡是借助 QQ 等第三方即时通信平台进行沟通的商家,一般都存在安全风险,因为目前知名的网店都具有独立完善的客户在线交流工具,通常不需要借助 QQ 等第三方即时通信平台来完成。

(2) 如果遇到由卖家通过 QQ 或邮件等方式主动发送来的链接,并称要求补办小额运费险、邮费时,一定要通过官方联系方式进行确认,不能轻信。一般情况下,如果存在小额运费险、邮费等服务,在用户购买商品时就有提示,不需要事后再提醒客户。

(3) 一旦遇到需要填写账号、密码、身份证号码等个人信息时,对网站的真实性一定要进行严格的审查和确认。必要时,也可以使用一些安全验证工具(如 360 安全浏览器的“网站”功能)对网站的真实性进行辨认。

7.5.3 购买违禁品骗局

信息技术是一把双刃剑,一方面信息技术带来的便利已惠及普通大众,另一方面利用信息技术的违法行为也在借助于互联网这一最大的信息平台得到蔓延,在一定程度上影响着人们生活的安全和社会的稳定。日前,在互联网上随处可见违法买卖仿真枪、违禁药品、窃听设备等现象,而且由这些违法行为还衍生出了一些网络诈骗行为。

1. 案例分析

浙江肖女士因怀疑自己在外地工作的丈夫有外遇,在朋友的介绍下,通过网络购买了一个手机卡监听器。根据网上产品介绍,只要把该手机卡监听器插入手机的 SIM 卡插槽,输入要监听的手机号码,就能够起到电话监听、短信拦截、卫星定位等作用。

肖女士通过网络搜索到了一款自认为功能不错的手机卡监听器(这类信息网络上随处可见,图 7-16 所示的便是随意搜索到的一个产品宣传和销售网站)。根据网上提供的联系方式,肖女士通过 QQ 与对方联系后,以 6000 元购得了该手机卡监听器。但当肖女士将买到的手机卡监听器插入自己的手机后,什么反应都没有,连电话也不能打。肖女士在联系了卖家后,卖家称要交 10 000 元的卡激活费。肖女士只得又汇款给对方,之后对方称还要交 9980 元购买一款专用手机。

这时,肖女士意识到自己可能被骗了,于是拒绝继续向对方汇款。但是,对方却声称:如果肖女士不照办,不但拿不到手机,还要通知她的丈夫。顾及和丈夫的关系,肖女士在知道已经上当受骗的情况下,还是将钱汇给了对方。然而,汇了这笔款后,对方又向肖女士提出支付高额封口费的要求。无奈之下,肖女士只得向警方报案。

在本案例中,不管肖女士购买的手机卡监听器能否正常使用,她的这一行为本身就是违法的。这种违法行为,不但买家知道,而且卖家早已明白。所以,卖家也是利用了买家受骗后不敢轻易声张这一弱点,对买家继续进行欺诈。这种通过购买违禁品后,再进行连环诈骗的现象,危害非常严重。

2. 主要防范方法

不法分子通过网络销售所谓的监听器,主要瞄准了用户的以下心态:一是急于窥视他



图 7-16 网上随处可见的出售监听设备的网站

人秘密；二是对设备缺乏必要的了解；三是受骗者通常不敢声张。另外，不法分子实际提供的设备，其功能根本不像网站上宣传的那么强大，多数情况下，甚至就不具备任何功能。例如，本案例中的手机卡监听器根本就没有监听功能。这样，即使被查处，也可以减轻法律责任。

不法分子运用“货到付款”的手段，诱使受骗者一步步误入陷阱。在到货后，又会以密码激活、开启 PIN 码等方式，继续诱骗受骗者不断给其汇款。其实，这类网购诈骗的防范方法很简单：一是不轻信网络广告，不猎奇；二是不做违法的交易。

习 题

1. 结合传统桌面互联网应用，试分析移动互联网的应用特点。
2. 以智能手机为例，说明移动终端的节能和定位功能。
3. 名词解释：移动搜索、移动社交网络、自媒体、隐私保护。
4. 什么是中间人攻击？结合移动互联网应用，试分析“中间人攻击”的防范方法。
5. 试分析软键盘的应用特点，如何防范针对软键盘应用的攻击？
6. 名词解释：逆向工程、二次打包、应用加固、签名验证。
7. 什么是双因子认证？什么是伪双因子认证？如何防范移动应用中的伪双因子认证？

8. 结合日常应用,试分析骚扰电话的一般特征以及防范方法。
9. 结合日常应用,试分析诈骗电话的一般特征以及防范方法。
10. 结合日常应用,试分析垃圾短信的一般特征以及防范方法。
11. 结合日常应用,试分析二维码的应用特点以及存在的安全问题,如何进行防范?
12. 什么是云计算? 云计算存在哪些应用风险? 如何防范?
13. 结合日常应用,试分析针对网络购物攻击的防范方法。

-
- [35] 张茜,延志伟,李洪涛,等.网络钓鱼欺诈检测技术研究[J].网络与信息安全学报,2017,3(7): 1-18.
- [36] 360 互联网安全中心.2016 年中国网站安全漏洞形势分析报告[EB/OL].(2018-01-05)[2018-06-09].<http://zt.360.cn/1101061855.php?dtid=1101062368&did=210133742>.
- [37] 梁雪松.IDN 欺骗行为及其防御技术研究[J].电脑知识与技术(学术交流),2007(5): 643-661.
- [38] 罗军舟,吴文甲,杨明.移动互联网:终端、网络与服务[J].计算机学报,2011,34(11): 2029-2051.

图书资源支持

感谢您一直以来对清华版图书的支持和爱护。为了配合本书的使用,本书提供配套的资源,有需求的读者请扫描下方二维码,在图书专区下载,也可以拨打电话或发送电子邮件咨询。

如果您在使用本书的过程中遇到了什么问题,或者有相关图书出版计划,也请您发邮件告诉我们,以便我们更好地为您服务。

我们的联系方式:

地址:北京海淀区双清路学研大厦 A 座 707

邮编:100084

电话:010-62770175-4604

资源下载:<http://www.tup.com.cn>

电子邮件:weijj@tup.tsinghua.edu.cn

QQ: 883604(请写明您的单位和姓名)

用微信扫一扫右边的二维码,即可关注清华大学出版社公众号“书圈”。

资源下载、样书申请



书圈